Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.49

스마트그리드 기기 보안 침해사고 대응을 위한 원격 증거 수집 시스템 설계*

강 성 구,† 김 신 규‡
한국전자통신연구원 부설연구소

The Design of Remote Digital Evidence Acquisition System for Incident Response of Smart Grid Devices*

SeongKu Kang,† Sinkyu Kim‡
The Attached Institute of ETRI

요 약

스마트그리드 기기는 스마트그리드의 주요 구성요소로 전력 서비스와 관련된 다양한 정보를 수집 및 처리하고, 주변의 다른 스마트그리드 기기 또는 상위 시스템들과 정보를 송·수신하여 보다 지능화된 전력 제공 서비스 제공한다. 하지만 이러한 스마트그리드 기기들은 보안 침해사고 발생 시 다른 스마트그리드 기기 또는 상위 주요 시스템으로 침입할 수 있는 경로로 활용될 수 있으며, 이로 인해 전력 서비스에 큰 장애가 발생 할 수 있다. 따라서 보안 침해사고 발생 시 전력 서비스의 가용성 확보를 위해 스마트그리드 기기에 대한 증거 수집 및 분석, 복구 등에 있어 보다 신속한 대응이 요구된다.

본 논문에서는 이러한 스마트그리드 기기에서 발생될 수 있는 보안 침해사고를 보다 신속하게 대응하기 위해 스마트그리드 기기의 운영환경을 분석하여 원격 증거 수집 시스템이 기존 IT환경에 비해 스마트그리드 환경에서 보다 효과적으로 적용 및 운영됨을 제시하였으며, 이를 바탕으로 스마트그리드 기기 운영환경을 고려한 스마트그리드 기기 원격 증거 수집 시스템 설계 방안을 제시하였다.

ABSTRACT

Smart Grid devices are the major components of the Smart Grid. They collect and process a variety informations relating power services and support intelligent power services by exchanging informations with other SG devices or systems. However, If a SG device is attacked, the device can provide attack route to attacker and attacker can attack other SG devices or systems using the route. It may cause problem in power services. So, when cyber incident is happened, we need to acquire and examine digital evidence of SG device quickly to secure availability of SG.

In this paper, we designed remote evidence acquisition system to acquire digital evidences from SG devices to response quickly to incidents of SG devices. To achieve this, we analyzed operating environment of SG devices and thought remote digital evidence acquisition system of SG devices will be more effective than remote digital evidence acquisition system targeted general IT devices. So, we introduce design method for SG devices remote evidence acquisition system considered operating environment of SG devices.

Keywords: Smart Grid, Smart Grid Devices, Incident Response, Digital Forensic, Remote Evidence Acquisition

접수일(2014년 10월 13일), 수정일(2015년 1월 22일), 게재확정일(2015년 1월 24일)

* 본 연구는 2014년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.(No. 201201050004A)

† 주저자, ssabro@ensec.re.kr
‡ 교신저자, skkim@ensec.re.kr(Corresponding author)

I. 서 론

스마트그리드 기기(이하 SG 기기)는 기존 전력망과 스마트그리드를 구분 짓는 주요 구성요소로 전력 서비스의 신뢰성과 질을 향상시키고, 최적화된 전력 생산, 전달, 소비 유도하여 전력 생상 및 제공에 효율성을 높이고, 시스템 장애를 신속히 복구 하는 등 보다 지능화된 전력 서비스 제공에 필요한 다양한 정보를 수집 및 처리하고, 필요 시 제어하는 기능을 담당한다[1].

대표적인 SG 기기로 스마트미터, 데이터집중장치(DCU, Data Concentration Unit), 홈게이트웨이, IHD(In-Home Display), 전기자동차 충전기, 대용량전력저장장치(ESS, Energy Storage System), 변전소지능형전력장치(IED, Intelligent Electronic Device) 등이 존재하며, 이러한 SG 기기는 기존 IT환경에서의 임베디드 기기들과 매우 유사한 시스템 구조 및 통신 환경을 가지고 있다.

따라서 SG 기기들은 기존 IT기술이 가지고 있는 다양한 보안 취약점들에 그대로 노출 될 수 있으며, 실제 SG 기기를 대상으로 한 보안 침해사고 사고사례들이 보고되고 있다[2-4].

이러한 SG 기기들이 보안 침해사고가 발생할 경우 연결되는 주변 SG 기기 또는 상위 시스템 침입할 수 있는 경로를 제공할 수 있어 전력 서비스 제공에 심각한 장애가 발생 될 수 있다.

따라서 보안 침해사고 발생 시 SG 기기에 발생한 보안 침해사고 내용과 그 원인을 명확히 분석하고 그 원인에 따라 적절한 대응이 이루어져야 할 필요가 있으며, 이를 위해 디지털 포렌식 기술을 활용한 증거 데이터 수집이 요구된다.

본 논문에서는 SG 기기 운영환경을 분석하여 디지털 포렌식을 위한 증거 데이터 수집 시 고려되어야할 요소들을 식별하고, 이를 만족할 수 있는 SG 기기 원격 증거 수집 시스템을 설계 및 구현한다.

Ⅱ장에서는 SG 기기 운영환경과 SG 환경에서 원격 증거 수집 적용에 대해 설명하고, Ⅲ장에서는 SG 기기 원격 증거 수집 시스템 설계 방안을 제시한 뒤, Ⅳ장에서 결론을 맺는다.

II. 배경 및 관련연구

2.1 SG 기기 운영환경 특성 분석

SG 기기 운영환경 분석을 통해 증거 수집 시 고려되어야할 요소를 살펴보면 Table 1.같이 요약할 수 있다.

SG 기기는 전력 서비스 특성상 무엇보다 가용성이 우선적으로 요구된다. 이로 인해 증거 수집 시 전통적인 방식의 네트워크 연결을 제한하거나 시스템의 전원을 종료한 뒤 증거 데이터를 수집하는 행위가 제한적일 수 있다. 또한, 이러한 특성으로 인해 침해사고 발생 시 보다 신속한 대응 및 복구가 이루어져야 한다. 단, 복구 시 침해사고 분석에 필요한 증거 데이터가 손실될 수 있기 때문에 복구를 실제 수행하기 전에 침해사고 발생 즉시 증거 수집이 이루어질 수 있도록 고려되어야 한다.

SG 기기는 다양한 기기 또는 시스템들과 유기적으로 상호 연결되어 운영되는 특성을 갖는다. 이러한 특성으로 인해 보안 침해사고 내용에 따라 사고가 발생된 SG 기기뿐만 아니라 대상 기기와 유기적인 관계를 갖는 기기 또는 시스템에 대한 조사가 필요할 수 있으며 이에 대한 지원이 고려되어야 한다.

SG 기기들은 많은 수의 기기들이 물리적으로 분산된 환경에 위치하여 운영되는 특성을 갖는다. 이에 따라 증거 조사자가 분석에 필요한 증거 데이터를 수집하기 위해 조사 대상 SG 기기가 설치되어 운영되는 현장에 직접 이동하여 수집하는데 많은 비용이 요구될 수 있어 이에 대한 고려가 필요하다.

또한, SG 기기들은 기기 특성 및 제조사에 의해 다

Table 1. Attribute operating environment of Smart Grid devices

	Attribute
1	Ensure availability
2	Rapid Recovery
3	A number of devices
4	The place where the physical distribution
5	Utilizing a variety of platforms
6	Utilizing Low capacity volatile and non-volatile storage
7	Support for IP-based communications interface

양한 형태의 플랫폼, 다양한 하드웨어 구성으로 개발 및 생산될 수 있다. 제주 스마트그리드 실증단지 구축 현황, 한전KDN, LS산전 등 국내 SG 기기들을 생산되는 제품들, 한국전력공사의 제품 규격서[5,6,7] 등을 살펴보면 생산되는 SG 기기들 중 일부 기기를 제외한 대부분의 기기는 실시간 운영체제 또는 범용 운영체제를 활용하고 있으며, 특히 최적화된 임베디드 리눅스 운영체제를 다양한 기기에 적용하여 활용 및 생산되고 있다. 하드웨어 규격을 살펴보면 128MB ~ 1GB 용량의 휘발성·비휘발성 저장매체를 사용하고 있으며, 이더넷, PLC(Power Line Communication), ZigBee, BCDMA 등 다양한 통신 인터페이스를 지원한다.

스마트그리드는 IEC, ISO, IEE, IETF, ANSI, ETSI, ITU-T 등의 표준화 기구들을 통해 상호운용성을 위한 표준화를 진행하고 있다. 스마트그리드와 관련된 대부분의 표준에서는 다양한 유·무선 매체의 사용한 통신 프로토콜로 인터넷 프로토콜(IP : Internet Protocol)을 기반으로 개발되고 있으며 SG 기기들은 이러한 프로토콜 지원을 위한 IP통신 인터페이스를 지원하고 있다[8,9].

2.2 원격 증거 수집 시스템

원격 증거 수집이란 원격지에 존재하는 시스템으로부터 온라인 기반에 증거 데이터를 수집하는 방법으로 현재 다양한 원격 증거 수집 시스템 솔루션이 존재한다[10]. 대표적으로 EnCase Enterprise, AccessData Enterprise, OnlineDFS, MacQuisition CF 등 이 존재하며, 주 대상 플랫폼으로 윈도우즈, 리눅스 및 유닉스, 맥OS를 대상으로 한다[11,12,13,14].

이러한 솔루션은 대부분 TCP/IP 기반의 서버, 클라이언트 구조를 가지며 구성은 서버와 에이전트로 구성된다. 서버와 에이전트는 각각 사용사례에 따라 서버와 클라이언트 역할을 모두 가질 수 있으며, 서버는 에이전트로 증거 데이터를 요청하거나 에이전트로부터 송신되는 증거 데이터들을 수신 및 관리하는 역할 갖는다, 에이전트는 대상 시스템에 설치되어 서버로부터 증거 데이터 요청이나 특정 보안 이벤트 발생 시 자신이 설치되어 있는 시스템으로부터 증거 데이터들을 수집하여 서버로 전송하는 역할을 수행한다. 증거 수집 시 raw 이미지 등 다양한 포맷으로 수집이 가능하며, 증거 전송 구간에 TLS(Transport Layer Security)을 적용하여 기밀성 및 무결성을 제공하고 서버를 인증을 수행한다, 추가적으로 증거 수집가를 ID, 패스워드 기반에 인증할 수 있는 보안 기능을 제공한다.

이런 원격 증거 수집 시스템은 Table 2.와 같은 장점을 제공한다.

원격 증거 수집 시스템은 기본적으로 증거 수집 대상 시스템에 에이전트가 설치되어 운영되는 형태로 시스템이 활성화 되어 있는 상태에서 증거 수집이 이루어진다. 따라서 시스템의 가용성을 보장할 수 있으며 비휘발성 증거 데이터뿐만 아니라 휘발성 증거 데이터 수집이 모두 가능하다.

보안 침해사고가 발생된 시스템이 식별 가능할 경우 해당 시스템의 에이전트로 증거 데이터 요청을 통해 신속한 증거 수집이 가능하며, 에이전트가 설치되어 있는 시스템들에 동시에 증거 데이터를 요청하여 다수의 시스템으로부터 증거 데이터를 동시에 수집할 수 있다.

증거 수집가가 물리적으로 시스템에 접근하여 증거 수집 시 소요되는 시간적, 금전적 비용을 원격지에서 수행함으로써 이에 대한 비용을 줄일 수 있다.

또한, 증거 수집가의 증거 수집에 기술적 숙달 정도에 비의존적일 수 있으며, 각 시스템의 플랫폼 특성에 맞는 에이전트를 설치 운영함으로써 보다 시스템 플랫폼에 독립적으로 증거 데이터를 수집할 수 있다.

하지만 원격 증거 수집 시스템은 이러한 장점에도 불구하고 에이전트, 네트워크, 시스템 등에서 장애가 발생할 경우 정상적인 증거 수집 행위가 제한될 수 있는 점과 원격 증거 수집 기능이 오용되어 추가적인 보안 위협이 발생하거나 특히 일반적인 IT환경의 경우 개인 사용자의 사생활을 침해할 수 있다는 점에서 국

Table 2. Advantages of remote evidence acquisition system

	Advantages
1	Ensure system availability
2	Rapid evidence acquisition
3	At the same time, to acquire evidence from a large number of system
4	Low costs for evidence acquisition
5	Independent on evidence collectors
6	Collect all of the volatile and non-volatile data
7	Independent on system plaform

외 및 국내에서의 도입 사례는 미비한 실정이다[15].

추가적으로 최근에는 증거 수집 대상인 휘발성, 비휘발성 저장 매체의 저장 용량이 점점 커짐에 따라 과거에 비해 증거 데이터를 수집하고 전송하는 비용이 높아지고 있다.

이로 인해 일반 IT환경에서의 PC, 서버, 모바일 기기 등의 시스템들을 대상으로 한 원격 증거 수집 시스템 적용에 있어 다소 어려운 부분이 존재하나, SG 기기를 대상으로 한 원격 증거 수집 시스템은 2.1절에서 분석된 SG 기기 운영환경 특성상 고려해야할 사항들을 대부분 만족 시킬 수 있을 뿐만 아니라, 시스템 및 네트워크의 가용성을 최우선으로 관리되는 만큼 일반적인 IT환경에 비해 특정 장애로 인한 증거 수집 행위가 보다 안정적으로 수행될 수 있다.

특히 스마트그리드의 경우 전력서비스 제공자가 직접 기기 및 네트워크에 대한 관리를 수행하며, 스마트미터 등 일부 기기를 제외한 나머지 기기들은 특정 사용자의 사생활을 직접적으로 침해할 수 있는 여지가 일반적인 IT환경의 시스템들에 비해 상대적으로 미비할 것으로 판단된다.

또한, 기존 IT환경의 시스템들에 비해 보다 작은 용량의 휘발성·비휘발성 저장매체를 사용하고 있어 증거 수집 및 전송 되는 비용이 보다 적게 소요될 것으로 예상된다.

따라서 SG 기기들을 대상으로 한 원격 증거 수집 시스템 도입이 기존 원격 증거 수집 시스템의 장점을 그대로 수용하고 기존에 가지고 있던 다양한 제약사항을 보다 최소화 할 수 있어 SG 기기를 대상으로 한 원격 증거 수집 시스템 적용이 보다 효과적이다 할 수 있다.

III. 시스템 설계

3.1 시스템 목표

SG 기기 원격 증거 수집 시스템의 목표는 Table 3.과 같다.

증거 수집가는 증거수집요청, 증거수집, 증거관리 및 제공 등 증거 수집 처리 과정 전반에 대해 그 과정을 제어할 수 있어야 하며 그 과정을 확인할 수 있어야 한다.

증거 수집 처리의 객관성과 신뢰성 확보를 위해 증거 요청 주체, 증거 수집 주체, 증거 관리 주체를 구분하고 각 과정에서 증거 수집 기능이 오용되지 않도록 요청 주체자의 권한을 확인할 수 있어야 한다.

Table 3. Goal of remote evidence acquisition system

	Goal
1	Control and verification of acquisition process
2	Provide independent of acquisition process
3	Provide authorization of acquisition process
4	Provide Integrity, reliability, originality, compatibility, confidentiality of acquisition data
5	Manage of devices status
6	Manage of devices relationship information

디지털 증거 특성상 위·변조가 용이하여 수집되는 증거에 대한 무결성과 신뢰성 확보가 무엇보다 중요하며, 대상 기기로부터 정확하게 수집되었는지 검증될 수 있어야 한다.

뿐만 아니라 수집된 증거 데이터에는 기기에 존재하는 모든 정보가 포함될 수 있어 위협원에 이러한 정보가 노출될 경우 심각한 보안문제가 발생 될 수 있다. 따라서 전송, 저장 및 관리 단계에서 기밀성이 보장되어야 한다.

증거 수집가는 신속한 증거 수집이 이루어질 수 있도록 원격지에 있는 기기 상태를 확인하여 원격에서 증거 수집이 가능한지 주기적으로 모니터링할 필요가 있으며, 침해사고가 발생한 기기 외에 추가적인 증거 수집이 필요할 수 있는 기기들을 식별하기 위해 SG 기기가 통신 또는 서비스상 관계되는 기기 또는 시스템 정보를 관리하여 필요 시 관련 기기들로부터 증거 데이터를 수집할 수 있어야 한다.

3.2 시스템 구조

SG 기기 원격 증거 수집시스템은 Fig. 1.과 같이 증거 수집 처리의 독립성을 제공하기 위해 증거수집에이전트(이하 EAA(Evidence Acquisition Agent)), 증거수집제어서버(이하 EACS(Evidence Acquisition Control Server)), 증거수집중계서버(이하 EARS(Evidence Acquisition Relay Server)), 수집증거관리서버(이하 EMS(Evidence

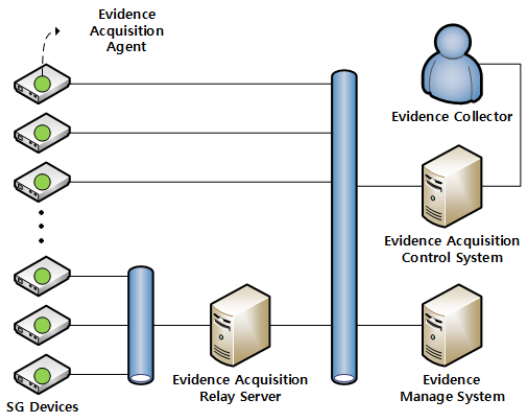

Fig. 1. Architecture of SG devices remote evidence acquisition system

Manage Server))로 그 기능을 나누어 구성한다.

EAA는 SG 기기에 설치되어 EACS에게 주기적으로 상태정보를 전송하여 연결 가능 여부를 알리는 기능을 제공한다. EAA는 EACS로부터 증거 데이터 요청을 수신하거나 SG 기기의 침해사고를 탐지할 경우 기기의 휘발성·비휘발성 증거 데이터를 수집하여 EMS로 전송하는 역할을 수행한다.

EACS는 EAA로부터 상태정보를 수신하여 원격에서 증거 수집이 가능한지 그 상태를 관리하고, 외부로부터 보안 침해사고 이벤트를 수신할 경우 증거 수집 요청을 위한 정보를 생성하여 EAA에게 직·간접적으로 증거 데이터 수집을 요청하는 기능을 수행한다. 또한, SG 기기와 직접적으로 연관되어 있는 다른 SG 기기와의 관계정보를 관리하여 추가적인 증거 데이터 수집이 필요한 대상을 식별한다.

EARS는 EAA와 EACS, EAA와 EMS 사이에 위치하여 상호 송·수신되는 정보를 전달하는 역할을 수행하며 상호간 직접적인 통신이 네트워크 구조 등의 이유로 불가할 경우 활용되며, 본 시스템은 필요 시 생략될 수 있다.

EMS는 EAA가 전송하는 증거 데이터를 수신 및 관리하고 필요 시 증거 데이터를 제공하는 기능을 수행한다.

3.3 시스템 운용 시나리오

SG 기기 원격 증거 수집 시스템은 Fig. 2.와 같은 운용 시나리오를 갖는다. 침해 탐지/차단 시스템 등 외부 침해사고 보고에 의해 보안 침해사고 발생 여부를 인지했을 경우 EACS에 의해 원격 증거 수집을 수행한다. 먼저, 탐지된 침해사고 정보로부터 증거 수집 대상이 어떤 SG 기기인지 식별한 한다. 이어 해당 SG 기기의 EAA가 운영되며, 접속 가능한 상태인지 확인한다. 접속이 가능할 경우 EACS는 '증거 수집 요청 데이터'를 작성한 뒤 EAA에게 직접 또는 EARS를 통해 증거 데이터를 요청한다. EAA는 EACS로부터 수신한 증거 수집 요청 정보가 적절한지, 증거 수집 요청자가 적절한 권한을 소유하고 있는지 검증하여 그 결과를 EACS에게 직접 또는 EARS를 통해 응답한다. 검증에 성공할 경우 EAA는 증거 데이터 전송을 위해 필요한 정보를 EMS와 직접 또는 EARS를 통해 정보를 교환하고, 교환된 정보를 바탕으로 증거 데이터 수집과 동시에 EMS로 전송한다. EAA는 전송을 완료한 뒤 수집 및 전송한 증거 데이터 정보를 활용하여 '수집 증거 데이터'를 작성한다. EAA는 작성한 '수집 증거 데이터'와 기존 EACS로부터 수신한 '증거 수집 요청 데이터'를 포함하여 EMS에게 직접 또는 EARS를 통해 증거 데이터 등록을 요청한다. EMS는 수신한 임시 증거 수집 데이터와 증거 등록 요청 정보와 비교 분석하여 그 정보가 적절한지, 등록 요청자가 적절한 권한을 소유하고 있는지 검증한다. 검증 성공 시 증거 수집 데이터를 저장 및 등록하고 그 결과를 EACS로 보고하여 증거 수집을 종료한다.

만약, 기기 자체에서 침해사고 발생 여부를 인지하여 증거 데이터를 수집 및 전송하는 경우 위 시나리오 중 EACS에 의한 증거 수집 요청 절차는 생략될 수 있다.

3.4 시스템 활용 데이터 및 데이터 검증

3.4.1 기기 상태 정보 데이터

기기 상태 정보 데이터는 EAA에 의해 생성되어 EACS로 전송되는 데이터로 기기정보와 시스템정보로 구성된다. 기기정보는 기기 종류, 제조사 등 기기의 기본적인 정보와 EAA에게 증거 수집 요청 시 네트워크 연결을 위해 필요한 정보를 포함한다. 시스템 정보는 EACS에게 최초로 기기 상태 정보를 전송하는 경우 또는 EACS의 요청에 의해 기기 상태 정보를 전송할 경우 포함하는 정보로 운영체제 정보 및 휘발성·비휘발성 저장매체의 기본 정보를 제공한다. EACS는 이러한 정보를 수신하여 에이전트 상태를

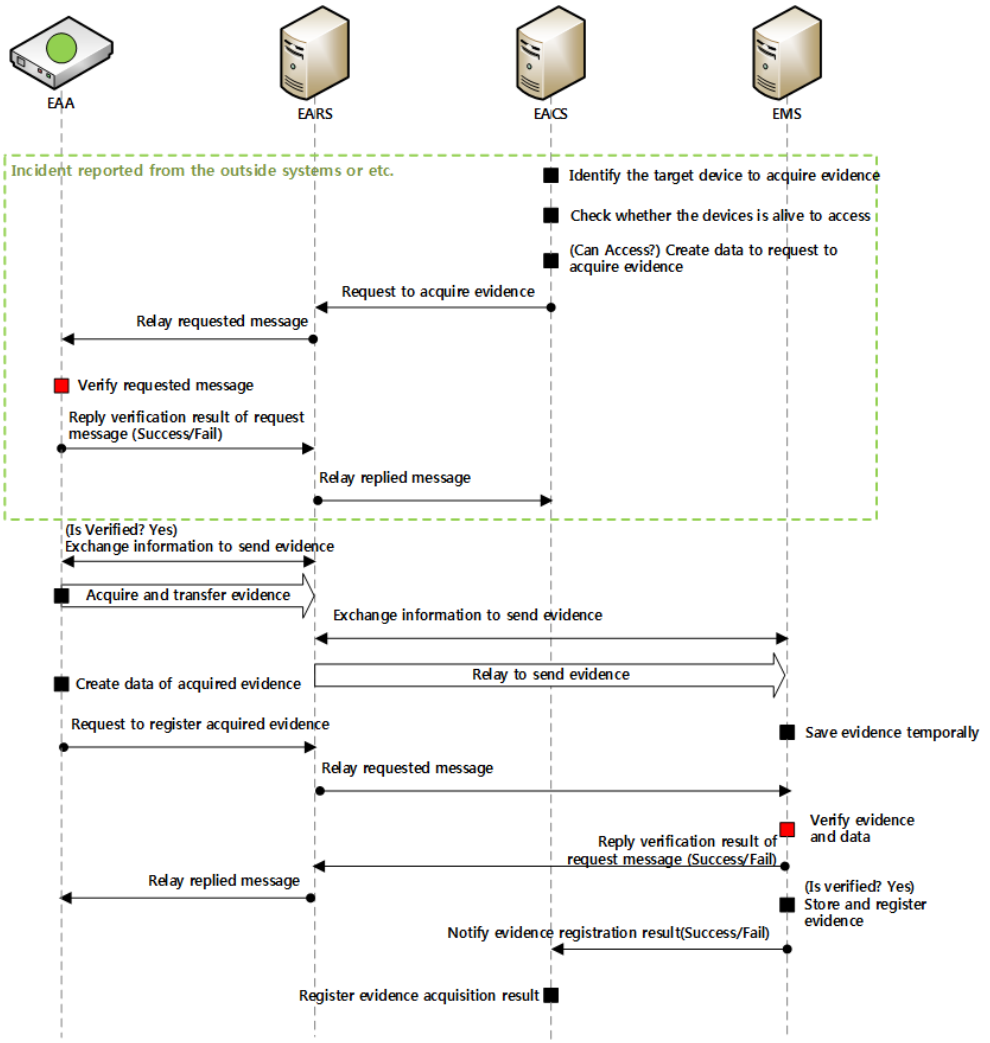

Fig. 2. Scenario of SG devices remote evidence acquisition system

관리하고, 기기 시스템 정보를 관리할 수 있다.

3.4.2 증거 수집 요청 데이터

증거 수집 요청 데이터는 EACS를 활용한 증거 수집가에 의해 생성 및 관리되는 데이터로 증거수집에이전트에게 증거 데이터를 요청하기 위해 필요한 정보를 포함한다.

증거 수집 요청 데이터는 기본정보, 사건정보, 대상정보, 서명정보로 구성되며 기본정보는 증거 수집 요청에 대한 설명 정보로 본 요청의 유효기간과 요청자의 정보를 포함한다. 사건정보는 증거 수집 요청에 대한 근거로 내·외부로부터 보고된 침해사고 정보를 표현한다. 대상정보는 실제 증거 수집 요청을 수신하여 처리해야할 대상 기기의 정보로 기기 상태 정보 데이터로부터 참조되어 작성된다. 서명정보는 증거 수집 요청에 대한 무결성을 보존하고 요청에 대한 부인방지 기능을 제공하기 위한 해시 및 서명 값이 포함되며 이와 관련한 파라미터 정보들이 포함된다.

EAA는 증거 수집 요청 데이터를 EACS으로부터 수신할 경우 다음과 같은 항목을 통해 요청 정보와 그 권한을 검증한다.

Table 4. Data of SG devices remote evidence acquisition system

Data	Group	Elements	Description	Req.	-
Device Status Information Data	Basic	device_id	accident occurred devices ID	O	
		type	devices type(ex, DCU)	O	
		maker	devices maker		
		model	devices model		
		ip	devices IP address	O	
		port	devices port number	O	
		location	devices physical location		
	System	host	devices host name	O	Optional
		os	devices OS name or type	O	
		version	devices OS version	O	
		processor	Processor Type	O	
		ram_size	size of volatile memory	O	
		disk_size	size of nonvolatile memory	O	
		MAC	MAC Address	O	
		datetime	current date time	O	
		uptime	alive operating time	O	
Evidence Acquisition Request Data	Basic	acquisition_id	acquisition ID	O	
		issued	acquisition issued datetime	O	
		expired	acquisition expire datetime	O	
		requestor	acquisition requestor ID	O	
	Case	case_id	case ID	O	
		risk	case risk level(ex, 1~5)	O	
		type	case type(ex, malware, unathorized, ...)	O	
		datetime	case event datetime	O	
		source	case source		
		desc.	case description		
	Target	equal "Basic" of "Device Status Information Data"		O	
	Signature	timestamp	signature time stamp	O	
		hash	hash value of acquisition data	O	
		sign	signature Value of hash value	O	
		signer	signer's certificate key	O	
Acquired Evidence Information Data	Basic	acquisition_id	acquisition ID	O	
		case_id	case ID	O	
		method	acquisition method	O	
		creator	creator ID	O	
	Evidence	type	evidence type(ex, volatile or nonvolatile)	O	Multiple
		datetime	acquisition date time	O	
		size	evidence size	O	
		format	evidence format(ex, raw, ewf, ...)	O	
		hash	hash value of evidence	O	
	Source	equal "Basic" of "Device Status Information Data"		O	
	Signature	timestamp	signature time stamp	O	
		hash	hash value of acquisition data	O	
		sign	signature Value of hash value	O	
		signer	signer's certificate key	O	

항목 1. 증거 수집 요청 데이터를 수신한 시간과 요청 정보의 기본정보 중 요청시간 및 만료시간과 상호 비교하여 요청이 유효한지 확인

항목 2. 대상정보 중 기기ID와 자신(기기)의 ID와 동일한지 확인

항목 3. 서명정보 중 서명자의 인증서가 유효한지 확인

항목 4. 기본정보 중 증거 수집 요청자의 ID와 서명정보 중 서명자 인증서의 ID가 일치하는지 확인

항목 5. 기본정보 중 증거 수집 요청자 ID가 증거 수집가로 등록된 ID인지 확인

항목 6. 서명정보 중 해시 값과 계산된 해시 값이 일치 한지 확인

항목 7. 서명정보 중 서명 값을 서명자 인증서의 공개키로 복호화한 값과 해시 값이 일치 한지 확인

3.4.3 수집 증거 정보 데이터

수집 증거 정보 데이터는 EAA에 의해 생성되는 정보로 EMS로 전송된 증거 데이터들에 대한 정보를 표현한다. 본 정보는 기본정보, 증거정보, 출처정보, 서명정보로 구성된다.

기본정보 중 증거 수집 요청 ID와 사건 ID는 EACS로부터 수신한 증거 수집 요청 데이터 정보를 참조하여 작성된다. 만약 기기 자체에서 탐지되어 증거 데이터를 수집 및 전송하는 경우 증거 수집 요청 ID와 사건ID는 'trap' 으로 설정한다. 또한 기본정보는 수집에 사용된 방법, 증거 생성자인 기기ID를 포함한다. 증거정보는 휘발성 또는 비휘발성 증거 데이터 인지 구분하며, 전송된 증거 데이터의 생성시간, 크기, 포맷 정보와 해시 값을 전송하여 무결성을 보장한다. 또한 증거 전송의 부인방지를 위해 서명정보를 두어 검증할 수 있도록 정보를 제공한다. EAA는 증거 데이터 전송이 완료 후 생성한 수집 증거 정보 데이터와 EACS으로부터 수신한 증거 수집 요청 데이터가 존재할 경우 모두 EMS에게 전송한다. EMS는 수신 정보를 바탕으로 수신한 증거 데이터를 다음과 같은 항목으로 검증 후 성공 시 증거 데이터를 등록한다.

항목 1. 수집 증거 데이터 증거 정보와 수신한 증거 데이터와 일치(크기, 해시 값) 한지 확인

항목 2. 수집 증거 데이터 서명정보 중 서명자 인증서가 유효한지 확인

항목 3. 수집 증거 데이터 서명정보 중 서명자 인증서ID와 기본정보 중 생성자ID와 동일한지 확인

항목 4. 수집 증거 데이터 서명정보 중 해시 값과 계산된 해시 값이 일치 한지 확인

항목 5. 수집 증거 데이터 서명정보 중 서명 값을 서명자 인증서의 공개키로 복호화한 값과 해시 값이 일치 한지 확인

EAA가 전송한 데이터 중 증거 수집가 요청에 의해 수집된 경우 EAA는 증거 수집의 근거가 되는 증거 수집 요청 데이터를 EMS로 전송한다. 수신한 EMS는 3.4.2절에 설명한 바와 같이 증거 수집 요청 데이터 검증을 수행한 뒤 다음과 같은 항목을 추가적으로 검증하여 최종적으로 증거 등록 여부를 결정한다.

항목 1. 증거 수집 요청 데이터 기본정보 중 요청 ID와 수집 증거 정보 데이터 기본 정보 중 요청ID와 동일한지 확인

항목 2. 증거 수집 요청 데이터 사건정보 중 사건 ID와 수집 증거 정보 데이터 기본 정보 사건ID와 동일한지 확인

항목 3. 증거 수집 요청 데이터 대상정보 중 기기 ID와 수집 증거 정보 데이터 기본 정보 생성자ID와 동일한지 확인

3.5 시스템 통신 프로토콜

SG 기기 원격 증거 수집 시스템의 통신 프로토콜은 확장성과 보안성을 제공하기 위해 IP기반 TLS(Transport Layer Security)를 전송계층으

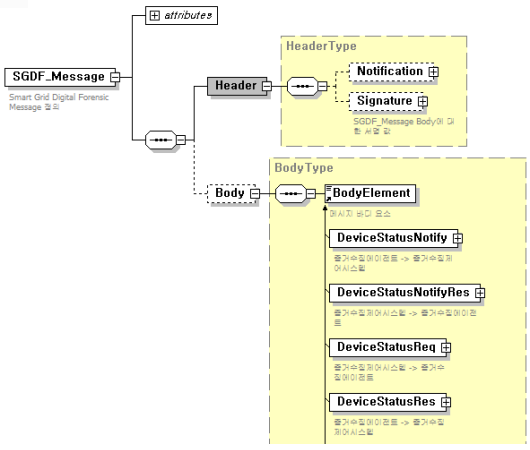

Fig. 3. SGDF Protocol XML Schema Definition

Table 5. SGDF Message Protocol body elements and description

	Elements Name	Sender	Receiver	Description
1	DeviceStatusNotify	EAA	EACS	notify status of device
2	DeviceStatusNotifyRes	EACS	EAA	reply about notification status of device
3	DeviceStatusReq	EACS	EAA	request status of device
4	DeviceStatusRes	EAA	EACS	reply status of device
5	EvidencesAcquisitionReq	EACS	EAA	request evidence acquisition
6	EvidencesAcquisitionRes	EAA	EACS	reply evidence acquisition
7	EvidencesTransferParameterReq	EAA	EMS	request parameter to transfer evidence
8	EvidencesTrasnferParameterRes	EMS	EAA	reply parameter to transfer evidence
9	EvidencesRegistrationReq	EAA	EMS	request evidence registration
10	EvidencesRegistrationRes	EMS	EAA	reply evidence registration
11	EvidencesRegistrationNotify	EMS	EACS	notify evidence registration result
12	EvidencesRegistrationNotifyRes	EACS	EMS	reply about notification evidence registration result

로, HTTP(Hyper Text Transport Protocol)를 응용계층으로 활용하고, 응용계층 전송 메시지 포맷은 XML 기반의 데이터를 활용한다. TLS는 TLSv1.2를 활용하고, “Certificate Request”옵션을 필수로 사용하여 통신 객체 간 상호인증이 수행될 수 있도록 처리한다.

응용계층 전송 메시지는 Fig. 3.과 같이 헤더와 바디로 구성되며, 헤더는 요청에 대상 설명, 요청에 대한 응답 코드를 포함하고 만약 응답 코드가 실패 일 경우 그 설명을 포함한다. 또한 메시지의 무결성과 부인방지를 위해 바디에 대한 해시 값 및 서명 값을 포함한다.

바디는 요청 또는 응답에 대한 실제 정보로 Table 5.와 같은 바디 엘리먼트들이 존재하며, 3.4 절에서 설명한 “기기 상태 정보 데이터”, “증거 수집 요청 데이터”, “수집 증거 정보 데이터”를 표현하여 송·수신한다.

Table 6.은 EACS에 의해 생성되어 EAA에 전송되는 증거 데이터 요청 메시지의 예로 메시지 바디에 “EvidencesAcquisitionReq” 엘리먼트를 가지며 “증거 수집 요청 데이터”를 “Order”로 표현하여 전송한다.

IV. 결 론

본 논문에서는 SG 기기에서 발생할 수 있는 보안 침해사고를 신속하게 대응하기 위해 원격에서 SG 기기 증거 데이터를 수집할 수 있는 시스템의 설계 방안에 대해 소개하였다. SG 기기 운영환경 분석을 통해 SG 기기를 위한 원격 증거 수집 시스템 적용 시 원격 증거 수집 시스템의 다양한 장점을 극대화 할 수 있을 것으로 기대되며, 원격 증거 수집 시스템의 한계들을 극복 또는 완화할 수 있어 SG 기기 환경 적용에 적합한 시스템으로 판단된다.

본 논문에서 제시한 SG 기기 원격 증거 수집 시스템을 통한 안전하고 신속한 증거 데이터 수집을 통해 향후 국가 단위 스마트그리드를 구축함에 있어 효과적으로 침해사고를 대응하는데 기여할 수 있을 것으로 판단된다.

향후, 제안된 설계 내용을 바탕으로 시스템을 구현 및 적용하여 안전성과 성능에 대한 검증이 필요하며, 본 시스템과 연동하여 보안 침해사고를 효과적으로 분석하고 추가적인 보안사고를 예방할 수 있는 연구 및 개발이 요구된다.

Table 6. EACS evidence acquire request message sample

```
<?xml version="1.0" encoding="UTF-8"?>
<SGDF_Message Version="1.0" xsi:noNamespaceSchemaLocation=SGDF_Message.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Header>
    <!-- Signature of Body-->
    <Signature SignAlgorithm="rsa" HashAlgorithm="sha256">
      <TimeStamp>2014-09-22T09:30:47Z</TimeStamp>
      <HashValue>.....</HashValue>
      <SignatureValue>.....</SignatureValue>
    </Signature>
  </Header>
  <Body>
    <EvidencesAcquisitionReq>
      <Order>
        <TokenID>T20140922-000001</TokenID>
        <GeneratorID>4a:b6:2f:c5:47:8e:40:81:a4:ad:b9:bd:4f:da:02:9f:eb:7f:07:c0</GeneratorID>
        <IssueDateTime>2014-09-22T09:30:47Z</IssueDateTime>
        <ExpireDateTime>2014-09-27T09:30:47Z</ExpireDateTime>
        <Use>acquisition</Use>
        <CaseInfo>
          <CaseID>C20140922-000001</CaseID>
          <RiskLevel>1</RiskLevel>
          <Category>Malicious Code</Category>
          <EventDateTime>2014-09-22T09:28:21Z</EventDateTime>
          <Source>SGIDS</Source>
          <Comment></Comment>
          <Status>registered</Status>
        </CaseInfo>
        <TargetDeviceInfo>
          <EAAID>a2:18:71:0b:3c:50:d0:b5:82:b9:70:fd:7e:8a:e1:1b:41:9b:e9:18</EAAID>
          <Type>DCU</Type>
          <Maker>DCU-Maker</Maker>
          <Model>DCU-Model</Model>
          <SerialNumber>D11223344</SerialNumber>
          <IPAddr>192.168.0.101</IPAddr>
          <ServicePort>8080</ServicePort>
          <PhysicalLocation>
            <Lat>37.50121</Lat>
            <Lon>127.03541</Lon>
          </PhysicalLocation>
        </TargetDeviceInfo>
      </Order>
      <!-- Signature of Order -->
      <Signature SignAlgorithm="rsa" HashAlgorithm="sha256">
        <TimeStamp>2014-09-22T09:30:47Z</TimeStamp>
        <HashValue>....</HashValue>
        <SignatureValue>.....</SignatureValue>
        <KeyInfo KeyType="x509"><!-- Certificate data of Generator -->
          <KeyValue>.....</KeyValue>
        </KeyInfo>
      </Signature>
    </EvidencesAcquisitionReq>
  </Body>
  </SGDF_Message>
```

References

〔1〕 NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0,", NISTSP 1108, May 2014,

〔2〕 IOActive, "OActive' Mike Davis to Unveil Smart Grid Research at Black Hat USA", IOActive press release, Jul. 2009.

〔3〕 Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies", Wall Street Journal, Apr. 2009.

〔4〕 Zoe Slocum, "Report: Smart-grid hankers could cause blackouts", CNN, Mar. 2009.

〔5〕 KEPCO, "Data Concentration Unit for Low Voltage AMI system", General Technical Specifications of KEPCO, GS-5895-0026, Jul. 2012.

〔6〕 KEPCO, "PLC Cel Bridge for low voltage Automatic Meter Reading", General Technical Specifications of KEPCO, GS-5895-0033, Jul. 2012.

〔7〕 KEPCO, "Feeder Remote Terminal Unit for LowVoltageDistribution Line Automation", General Technical Specifications of KEPCO, GS-5895-0028, May 2011.

〔8〕 IEC, "Communication networks and systems in substations Part 7-1: Basic communication structure for substation and feeder equipment. Principles and Models", IEC 61850-7-1, Jul. 2011.

〔9〕 ISO/IEC "Road vehicles- Vehicle to grid communication interface-Part 1:General information and use-case definition", ISO/IEC 15118-1

〔10〕 Jacob Pennock, Damon Smith, and Geoffrey Wilson, "Design and Implementation of a Remote Forensic System", Foundstone, http://www.foundstone.com

〔11〕 Encase Enterprise Edition, http://www.guidancesoftware.com/products/ee_index.aspx

〔12〕 AD Enterprise, http://www.accessdata.com/solutions/digital-forensics/ad-enterprise

〔13〕 OnLineDFS, http://www.cyberstc.com/products_dfs.asp

〔14〕 MacQuisition, https://www.blackbagtech.com/software-products/macquisition.html

〔15〕 Bora Park, Mina Shimm, and Sangjin Lee, "The Necessity of Remote Digital Forensic System Construction in Company", Review of KIISC, 18(1), pp.20-28, Feb. 2008.

〔16〕 NIST, "Guidelines for Smart Grid Cyber Security," NISTIR 7628, Sep. 2014.

〈저자소개〉

사 진

강 성 구 (Seongku Kang) 정회원
2008년 2월: 충남대학교 컴퓨터공학과 졸업
2011년 2월: 충남대학교 컴퓨터공학과 석사
2010년 2월~2011년 2월: 한국인터넷진흥원 주임연구원
2011년 3월~현재: 한국전자통신연구원 부설연구소 연구원
〈관심분야〉 스마트그리드 보안, 침해사고 대응, 디지털 포렌식

사 진

김 신 규 (Sinkyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2014년 2월: 연세대학교 컴퓨터과학과 박사
2003년 12월~현재: 한국전자통신연구원 부설연구소 선임연구원/실장
〈관심분야〉 스마트그리드 보안, 국가기반시설 보안, 취약점 분석