정 보 보 호 학 회 지
제24권 제5호, 2014. 10

보안 침해사고 대응을 위한 스마트 미터 로그 생성 및 수집 방안

강 성 구*, 김 신 규*

요 약

지구 온난화에 대한 대응 노력으로 국내·외적으로 스마트그리드가 주목받고 있다. 스마트그리드는 기존의 전력시스템과 IT기술을 접목하여 지능화된 전력시스템으로 스마트 미터는 이러한 스마트그리드의 핵심 구성요소라 할 수 있다. 하지만 이러한 IT기술이 융합됨으로 인해 스마트 미터는 기존 IT기술이 가지고 있던 보안위협을 그래도 상속받을 수 있으며 이로 인한 다양한 보안침해사고들이 발생될 수 있다. 스마트 미터에서 발생할 수 있는 보안 침해사고를 조기에 발견하고 대응할 수 있는 기초자료로 로그정보가 활용될 수 있지만 현재 스마트 미터와 관련한 로그 관리 방안이 부재한 것이 사실이다. 따라서 본 논문에서는 스마트 미터의 특성을 고려한 보안 침해사고에 대응할 수 있는 로그 생성 및 수집하여 추후 침해사고 대응 시 활용할 수 있는 방안을 제시한다.

Ⅰ. 서 론

스마트그리드는 기존 전력망에 IT 기술을 활용하여 전력공급자와 소비자 간에 실시간으로 전력 관련 정보를 양방향으로 교환 및 활용함으로써 에너지 효율성을 증진시키기 위한 융합 기술이다. 스마트 미터는 이러한 스마트그리드를 구현하기 위한 핵심기기로서 전력사용량을 측정하고 관리하는 기능을 수행한다. 스마트 미터는 기본적으로 실시간으로 사용된 전력량을 측정 및 저장하고 특정주기, 또는 특정 요청을 수신하였을 경우 측정된 데이터를 요청자에게 제공하는 역할을 수행한다. 서비스 제공자는 수신한 정보를 바탕으로 실시간 에너지수요량을 측정하고 실시간 가격 정책에 적용하고 전력을 보다 탄력적으로 생산하거나 부하를 제어할 수 있다. 사용자는 자신이 사용한 전력량과 실시간으로 제공되는 가격정보를 바탕으로 능동적으로 전기 사용 효율화에 참여할 수 있다.

국내에서는 에너지 비용의 감소, 신재생에너지 발전의 확대 여건 마련 및 수출산업화 등 국제경쟁력 확보를 위해 전략적으로 추진하고 있다. 최근 제주도 구좌읍에서 스마트그리드 실증단지 사업이 추진되었으며 2010년 기술 실증을 시작으로 2030년까지 스마트그리드 시스템 구축을 완료할 계획을 가지고 있다. 특히 국내 스마트 미터 보급은 2020년까지 국가 전체 가구에 보급할 계획을 가지고 있으며 지식경제부는 경제형, 일반형의 스마트 미터 보급을 예정하고 있다[1,2].

이러한 스마트 미터는 일반적으로 소비자 영역에 설치되어 운영되며 PLC, ZigBee 등과 같은 다양한 IT환경에서 활용된 통신기술을 사용함으로써 기존 미터 기기와 달리 다양한 보안위협에 노출될 수 있다. 실제 2009년 4월 미국 CNN은 스마트 미터의 취약점을 이용하여 스마트 미터가 쉽게 장악될 수 있음을 경고했으며 같은 해 7월 미국에서 열린 보안컨퍼런스 블랙햇(Black Hat)에서 미 보안 컨설팅 업체인 IOActive가 스마트 미터 펌웨어 업그레이드 취약점을 이용하여 악성코드를 전파할 수 있음을 발표하였다[3,4].

일반적인 정보시스템에서 보안 침해사고가 발생될 경우 이에 대한 원인을 분석하고 공격자를 추적하기 위해 정보시스템에 기록되어 있는 로그 정보가 활용되고 있다. 로그는 시스템이 수행한 행위들을 기록하는 것으

본 연구는 2014년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No.2012101050004A)

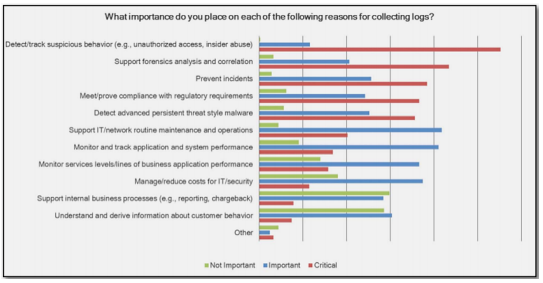
* ETRI 부설연구소 (ssabro@ensec.re.kr, skkim@ensec.re.kr)

로 이러한 정보를 통해 해당 정보시스템에 공격자가 수행한 행위를 추적하거나 공격으로 인해 발생된 시스템 피해를 파악하는 등에 보안 침해사고에 대한 후속조치를 수행하는데 중요한 근거가 될 수 있다. 하지만 현재 스마트 미터의 경우 보안 침해사고 대응에 활용될 수 있는 로그 생성 기준에 대해 명확히 정의된 내용이 없으며 이를 수집하기 위한 방안 또한 부재한 상황이다. 따라서 스마트 미터 보급에 앞서 스마트 미터의 로그 생성 방안과 로그를 안전하게 수집할 수 있는 방안이 요구되며 본 논문에서는 스마트 미터에 요구되는 로깅 대상들을 스마트 미터 사용사례를 통해 알아보고 스마트 미터환경에 적합한 로그 수집 방안을 제시한다.

본 논문의 구성은 2장에서 스마트 미터 로그의 필요성을 언급하고 3장에서는 스마트 미터의 특성 및 사용사례를 분석한다. 4장에서는 스마트 미터 환경에 적합한 로그 생성 및 수집 방안을 제시하며 5장에서 결론을 맺는다.

Ⅱ. 스마트 미터 로그의 필요성

로그는 정보시스템에서 발생되는 행위들을 기록하는 데이터로 시간정보를 기반으로 작성된다. 이러한 로그는 시스템에서 발생되는 오류나 접속한 사용자 등의 행위 등을 파악하여 보다 나은 서비스를 제공하기 위한 자료로 활용될 수 있다. 특히 보안 침해사고가 발생하였을 경우 항공기의 블랙박스와 같은 역할 수행하여 공격행위를 추적할 수 있는 핵심적인 증거자료로 활용될 수 있다. 실제 그림 1과 같이 보안 측면에서의 접속기록, 계정전환 등이 기록된 로그들을 수집 및 활용하고 있음을 알 수 있다[5]. 이러한 로그를 수집 및 분석함으로



〔그림 1〕 로그 수집 이유[5]

써 해당 시스템에 특별한 이상 징후는 없었는지 파악할 수 있으며 정기적인 취약성 진단과 병행하여 보안 침해사고 대책마련에 활용될 수 있다.

로그 관리는 컴플라이언스(Compliance)를 만족하기 위해 요구된다. 컴플라이언스란 내부통제 및 위험관리를 위한 것으로 국내에서는 '준법감시' 제도로 불린다. 이러한 컴플라이언스는 정보시스템의 구축 및 운영에 관련된 법령, 지침 등의 형태를 의미하며 전자적 기록물을 포함하여 보관, 책임 지정, 사용을 위한 접근기록을 보관하도록 명시하고 있다. 로그도 하나의 전자적 기록물로 분류될 수 있으며 로그와 관련된 국내·외 컴플라이언스들은 표 1과 같이 제시되고 있다[6].

미국의 표준화기관인 NIST(National Institute of Standard and Technology)는 2010년 8월 'NISTIR 7628 스마트그리드 사이버 보안 가이드라인'을 통해 스마트그리드에 대한 사이버 보안 요구사항을 명세하고 있다. 본 가이드라인을 통해 스마트그리드 환경에 존재하는 논리적 객체와 인터페이스를 식별하였으며 스마트미터와 관련된 인터페이스와 더불어 모든 인터페이스에 대해 표 2와 같은 보안감사에 대한 요구사항을 만족하도록 명시하고 있다[7].

〔표 1〕 로그관련 IT 컴플라이언스

구분	내용	비고
공공기관의 개인정보보호에 관한 법률	개인정보 이용에 대한 로그 필요성 명시	한국
정보통신망 이용촉진 및 정보보호 등에 관한 법률	개인정보 이용 및 제공에 대한 로그 필요성 명시	한국
공공기관 정보시스템 운영가이드라인	정보시스템 이용 내역 및 기록의 보관 내용 명시(6개월 이상 보관, 주1회 분석)	한국
ISO 27001	감사로깅, 로깅정보의 보호, 관리자/운용자 로그, 시간 동기화 명시	국제표준
HIPPA	병원이나 의료관련기관에 보관되어 있는 의료기록 및 건강 정보에 대한 자료관리 규제, 로그데이터 6년 보관명시	미국

〔표 2〕 로그관련 NISTIR 7628 보안요구사항

요구사항 번호 및 이름	설명
SG.AU-1. 보안감사 및 책임추적성 정책 및 절차	보안감사 및 책임추적성을 위한 정책 및 절차를 구현해야 한다.
SG.AU-2. 보안감사 이벤트	보안감사를 위해 정보시스템에 대한 이벤트를 식별해야 한다.
SG.AU-3. 보안감사기록 콘텐츠	감사기록(로그생성)시 기록되어야 하는 이벤트는 데이터 및 시간, 발생된 시스템 식별 정보, 이벤트 타입, 사용자 및 객체 ID, 이벤트 결과 등이 포함되어야한다.
SG.AU-4. 보안감사 저장 능력	각 시스템의 저장능력을 고려하여 감사 기록이 유실되지 않도록 관리해야 한다.
SG.AU-5. 보안감사 처리 실패 대응	보안감사 처리에 대한 실패 시 지정된 관리자에 통보되어야 하며 필요 시 시스템 정지, 과거 감사 기록 삭제, 기록 생성 정지 등 미리 정의된 행위를 수행해야 한다.
SG.AU-6. 보안감사 모니터링, 분석, 보고	부적절한 이상 행위를 모니터링하고 발생될 경우 보안감사 기록을 분석해야 하며 절차에 따라 보고되야 한다.
SG.AU-7. 보안감사 요약 및 보고서 생성	정보시스템은 감사 요약 및 보고서 생성을 지원해야 한다.
SG.AU-8. 타임스탬프	정확한 시간 정보 관리를 위해 내부의 관리시스템과 주기적으로 동기화를 수행해야 한다.
SG.AU-9. 보안감사 정보의 보호	불법적인 접근, 수정, 삭제 등으로부터 보안감사 정보를 보호해야 한다.
SG.AU-10. 보안감사 레코드 보존	정보시스템은 정한 기간 동안 보안감사 데이터를 안전하게 보호 및 관리해야 한다.
SG.AU-11. 보안감사의 조합 및 주기	보안요구사항 및 법, 규정에 적합한 주기별 조합해야 한다.
SG.AU-12. 감사관의 자격	정보시스템 운영환경, 감사에 포함되는 위험, 사이버 보안 및 정보시스템 정책과 절차에 대한 이해가 요구된다.
SG.AU-13. 보안감사 도구	보안감사 시 오용 및 오류 등이 발생되지 않는 증명된 도구를 사용해야 한다.
SG.AU-14. 보안정책 준수	정보시스템이 기관의 보안 정책에 준수 여부를 확인될 수 있도록 해야 한다.
SG.AU-15. 보안감사 생성	정보시스템은 감사에 필요한 이벤트 리스트에 대해 감사기록을 생성해야 한다.
SG.AU-16. 부인방지	정보시스템은 특정 행위 시 거짓된 부인에 대처할 수 있어야 한다.

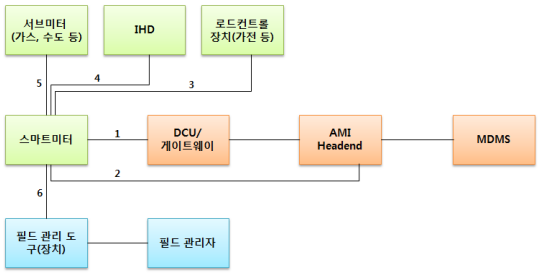
이처럼 스마트 미터에서의 보안 침해사고를 예방 및 대응하고 관련된 컴플라이언스 만족과 제시되고 있는 보안요구사항을 만족하기 위해 스마트 미터는 로그를 생성 및 관리될 필요가 있다.

Ⅲ. 스마트 미터 특성 및 사용사례 분석

3.1. 스마트 미터 운영환경 및 특성 분석

스마트 미터는 양방향 통신을 가능하게 하는 통신 모듈을 탑재한 계량기로서 AMI의 가장 기본적인 구성요소이다. AMI에 대한 논리적 아키텍처를 간략화 하면 그림 2와 같다.

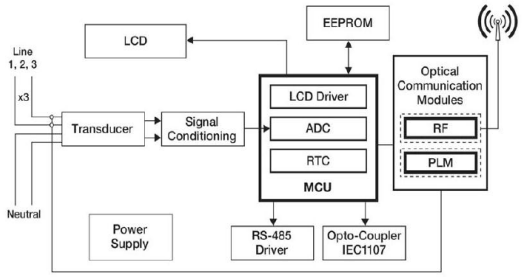
스마트 미터는 기본적으로 검침정보를 최종적으로 서비스 제공자의 MDMS(Metering Data Management System)에게 전송해야하는 역할을 가지고 있다. 이를 위해 스마트 미터는 1)과 같은 DCU 또는 게이트웨이와의 인터페이스를 가질 수 있으며 이를 통해 AMI Head-End로 전송할 수 있다. 또한 필요에 따라 AMI Head-End로 직접 전송할 수 있는 2)와 같은 인터페이스를 가질 수 있다. 스마트 미터는 가정 내 설치되어 있는 TV, 냉장고 등의 전력 부하원을 제어하기 위해 3)과 같은 인터페이스를 가질 수 있으며 사용자에게 전력사용량 정보 등을 제공하기 IHD(In-Home Display)와 4)와 같은 인터페이스를 가질 수 있다. 그 외 필요에 따라 전력 외에 가스, 수도 등의 사용량을 검침하는 서브미터와 5)와 같은 인터페이스를 가질 수 있으며 3) 및 5) 인터페이스는 서비스 제공자에 따라 인터페이스 유무가



〔그림 2〕 AMI의 논리적 아키텍처

결정될 수 있다. 또한, 서비스 제공자는 스마트 미터 관리를 위한 목적으로 필드 관리자가 물리적으로 접근하여 관리할 수 있는 필드 관리 도구를 제공할 수 있으며 스마트 미터는 이러한 도구와 통신을 할 수 있는 6)과 같은 인터페이스를 가질 수 있다[8].

스마트 미터가 가지고 있는 대부분의 인터페이스는 현재 전력선을 사용하는 PLC(Power Line Communication), 저전력의 근거리 통신에 주로 사용되는 ZigBee를 통신매체로 사용하고 있으며 필드 관리 도구와의 인터페이스의 경우 주로 RS485 또는 적외선 통신매체를 사용하는 것으로 파악되고 있다. 스마트 미터의 하드웨어 구성을 살펴보면 그림 3과 같이 일반적으로 8bit, 16bit 또는 32bit 마이크로컨트롤러(MCU)가 사용된다. 스마트 미터 애플리케이션을 위한 MCU의 경우 일반적인 반도체 전기미터용 MCU 제품에 요구되는 사항(예: 32KB 플래시 메모리, 2KB RAM 및 간단한 에너지 펄스 출력)보다 많은 것들이 충족될 수 있도록 요구되고 있으며 비용을 추가로 부담하지 않으면서 스마트 미터를 지원하기위해 스마트 미터 MCU에는 최소한 SPI 인터페이스, 64KB 플래시, 4KB RAM, 2개의 하드웨어 UART 및 캘린더 기능이 있는 하드웨어 RTC(Real Time Clock)가 요구되고 있다[9].



〔그림 3〕 스마트 미터 블록 다이어그램

3.2. 스마트 미터 사용사례 분석

위에서 언급한 AMI 논리적 아키텍처로부터 스마트 미터와 직접적인 관계를 갖는 인터페이스는 총6개이며 각 인터페이스에서 발생될 수 있는 사용사례를 살펴보면 표 3과 같다.

공통적으로 각각의 인터페이스는 보다 안전한 통신 채널 생성 및 서비스 제공을 위해 상호인증을 수행하는 사용사례가 있을 수 있다. 인터페이스 1에서의 DCU/게

〔표 3〕 스마트 미터관련 사용사례

IF. No.	구분	사용사례 및 정보
1	→ DCU/게이트웨이	A1. 상호인증 수행(인증정보)
	→ 스마트 미터	B1. 상호인증 수행(인증정보)
2	→ AMI Head-End	A1. 상호인증 수행(인증정보) A2. 미터링 데이터 요청 응답(미터링 데이터) A3. 스마트 미터 명령(on/off) 수행 응답 A4. HAN(Home Area Network) 연결 정보 전송 A5. 펌웨어 업데이트 수행 응답 A6. 서브 미터링 데이터 전달(서브 미터링 데이터) A7. 주기적 미터링 데이터 전송(미터링 데이터)
	→ 스마트 미터	B1. 상호인증 수행(인증정보) B2. 미터링 데이터 요청 B3. 스마트 미터 명령(on/off) 수행 요청 B4. 전력 가격정보 전달 B5. 전력 공급 정책(스케줄 등) 정보 전달 B6. 펌웨어 업데이트 수행(펌웨어 정보) 요청
3	→ 로드컨트롤 장치	A1. 상호인증 수행(인증정보) A2. 로드 컨트롤 시작 및 종료 이벤트 알림 전달 A3. 사용자 로드 컨트롤 명령 전달
	→ 스마트 미터	B1. 상호인증 수행(인증정보) B2. 로드 컨트롤 시작 및 종료 이벤트 알림 확인 응답 B3. 로드 컨트롤 명령 전송 응답
4	→ IHD	A1. 상호인증 수행(인증정보) A2. 전력 가격정보 전달 A3. 에너지 사용정보 전달 A4. 전력 공급 정책(스케줄 등) 정보 전달 A5. 로드 컨트롤 시작 및 종료 이벤트 알림 확인 응답 전달
	→ 스마트 미터	B1. 상호인증 수행(인증정보) B2. 로드 컨트롤 시작 및 종료 이벤트 알림 전송 B3. 사용자 로드 컨트롤 명령 전송
5	→ 서브 미터	A1. 상호인증 수행(인증정보)
	→ 스마트 미터	B1. 상호인증 수행(인증정보) B2. 서브 미터링 데이터 전송(서브 미터링 데이터)

IF. No.	구분	사용사례 및 정보
6	→ 필드 관리 도구	A1. 상호인증 수행(인증정보) A2. 미터링 데이터 요청 응답(미터링데이터) A3. 스마트 미터 명령(on/off) 수행 요청 응답 A4. AMI 시스템 등록 결과(성공) 전송 A5. 스마트 미터 통신진단 및 자가진단 요청 응답
	→ 스마트 미터	B1. 상호인증 수행(인증정보) B2. 미터링 데이터 요청 B3. 스마트 미터 명령(on/off) 수행 요청 B4. 스마트 미터 환경설정 데이터 전송 B5. 스마트 미터 통신진단 및 자가진단 요청

이트웨이는 장치 공급자에 따라 다양한 기능을 수행할 수 있도록 설계 및 개발될 수 있지만 본 논문에서는 네트워크 레벨에서 데이터 패킷을 스마트 미터와 AMI Head-End 간에 단순 송·수신하는 역할로 한정하였다.

Ⅳ. 스마트 미터 환경에 적합한 로그 생성 및 수집 방안

로그 생성 단계에서 고려되어야할 요구사항으로는 먼저 시스템 접속기록, 시스템 오류 이벤트 등 로그가 생성되어야할 항목을 정의할 필요가 있으며 생성될 경우 원인분석을 위해 어떠한 내용이 포함되어야 하는지 고려해야할 필요가 있다. 또한 실제 침해사고가 발생될 경우 다양한 시스템에서 생성된 로그와 통합하여 분석하는 경우가 있으므로 표준화된 로그 포맷과 시간동기화가 요구된다. 로그를 필요에 따라 수집을 해야 할 경우 관리자 등에 의해 임의적인 위·변조가 되지 않도록 무결성을 보장해야하며 로그에 사용자의 민감한 정보가 있을 수 있으므로 기밀성이 요구된다. 또한 명확하게 로그 데이터가 저장되었는지 보증되어야할 필요가 있다. 따라서 본 장에서는 이러한 요구사항을 만족하는 스마트 미터 로그 생성 및 수집 방안을 설명한다.

4.1. 스마트 미터 로그 생성항목 및 콘텐츠 분석

위에서 분석한 스마트 미터 사용사례들을 통해 스마트 미터에서 수행되는 행위들을 식별할 수 있다. 위 사용사례들 중 그 행위가 유사한 사용사례들을 정리하면 표 4와 같이 분류 될 수 있다.

‘인증’은 스마트 미터와 다른 시스템 간에 상호 정당한 시스템인지 확인하는 작업이 통신이 실제 수행되기 이전에 수행되어 질것으로 판단된다. 이러한 ‘인증’은 모든 인터페이스에서 수행되어지고 유사한 방식의 인증 방식이 사용될 것으로 판단된다. ‘요청’은 스마트 미터에게 직접적인 정보 요청하는 사용사례들을 의미하며 AMI Head-End와 필드 관리 도구에 의해 수행된다. ‘응답’은 스마트 미터가 수신한 정보 요청에 대한 응답을 수행하는 사용사례들을 의미하며 AMI Head-End 및 필드 관리 도구가 요청한 정보를 응답하게 된다. ‘전송’은 특별한 요청 없이 스마트 미터가 스스로 특정 이벤트 등이 발생되었을 경우 정보를 전송하는 사용사례들을 의미한다. ‘전달’은 스마트 미터가 정보전달에 있어 중계 역할을 수행하는 사용사례들을 의미하며 IHD와 로드컨트롤장치, IHD와 AMI Head-End, 서브미터와 AMI Head-End에 위치하여 정보 송·수신을 수행하게 된다.

위와 같은 행위에 대해 로그 생성 시 표현되어야할 콘텐츠와 로그 필수 여부를 정리하면 표 5와 같다.

기본적으로 로그 생성 시 반드시 요구되는 콘텐츠 정보는 시간정보이다. 이러한 시간정보는 상위시스템과 동기화된 시간정보를 바탕으로 생성되어야 하며 행위가 발생된 시점의 시간정보를 활용해야 한다. 각 행위들은 정상적인 수행이 이루어지거나 실패할 수 있으며 실패 시 이에 대한 근거를 표현할 필요가 있다. 실패는 통신 두절과 같은 네트워크 레벨에서의 문제가 있을 수 있으며, 필요한 정보가 부재하거나 시스템상에서의 문제, 접근권한 등의 보안문제 등으로 발생될 수 있다. 실패 원인은 발생된 사고 원인 등을 추적할 시 매우 유용한 정

〔표 4〕 스마트 미터에서의 유사 사용사례 분류

행위 유형	사용사례 번호 (ex, 인터페이스번호-사용사례번호)
인증	1-A1, 1-B1, 2-A1, 2-B1, 3-A1, 3-B1, 4-A1, 4-B1, 5-A1, 5-B1, 6-A1, 6-B1
요청	2-B2, 2-B3, 2-B6, 6-B2, 6-B3, 6-B5
응답	2-A2, 2-A3, 2-A5, 6-A2, 6-A3, 6-A5
전송	2-A4, 2-A7, 6-A4, 6-B4
전달	2-A6, 2-B4, 2-B5, 3-A2, 3-A3, 3-B2, 3-B3, 4-A2, 4-A3, 4-A4, 4-A5, 4-B2, 4-B3, 5-B2

〔표 5〕 행위 유형별 로그 생성 콘텐츠

행위 유형	콘텐츠 정보	필수
인증	시간정보, 인증대상 식별 정보(ex, ID or IP주소 등), 인증결과(성공, 실패), 실패 시 근거	O
요청	시간정보, 요청자 식별 정보, 요청정보	O
응답	시간정보, 응답대상 식별 정보, 요청정보, 응답결과(성공, 실패), 실패 시 근거	O
전달	시간정보, 전달 요청자 식별정보, 전달 대상자 식별정보, 전달정보, 전달결과(성공, 실패), 실패 시 근거	-
전송	시간정보, 전송대상 식별정보, 전송정보, 전송결과(성공, 실패), 실패 시 근거	O

보가 될 수 있으므로 다양한 실패 사례들을 고려하여 명확히 표현될 필요가 있다. '인증'은 실제 통신이 이루어지기 전에 수행되며 인증 대상과 인증결과 정보가 요구된다. 이러한 정보를 통해 부정하게 인증을 시도하는 객체를 식별하거나 통신이 정상적으로 이루어지지 않을 경우 그 원인을 파악하는데 도움이 될 수 있다. '요청'은 외부 객체로부터 스마트 미터에게 어떠한 정보를 요청했는지 파악할 수 있는 정보를 제공할 수 있다. 이를 통해 부정하게 요청한 객체를 식별하는 등에 정보를 제공할 수 있으며 응답은 스마트 미터가 외부 객체로 수신한 요청에 대해 어떠한 행위를 수행했는지 정보를 제공할 수 있다. '전달'은 스마트 미터에게 전달을 요청한 대상과 그 전달을 수신할 대상이 존재하므로 이에 대한 정보가 반드시 요구되며 '전송'은 스마트 미터가 전송한 정보와 그 대상에 대한 정보가 요구된다. '인증', '요청', '응답', '전송'과 같은 행위들은 스마트 미터에 존재하는 정보를 바탕으로 수행되는 행위들이며 스마트 미터 운영에 직접적인 관계를 가지고 있으므로 로그에 대한 기록이 필수로 요구된다. '전달'의 경우 다른 행위들과 다른 시스템과 다른 시스템간에 정보교환 역할만을 수행하므로 서비스 제공자 등에 의해 선택적으로 기록될 수 있을 것으로 판단된다.

위 사용사례 분석을 통한 스마트 미터의 행위 외에 시스템 레벨에서 발생될 수 있는 다양한 이벤트들이 존재할 수 있다. 대표적으로 시스템이 부팅 및 종료 등이 있을 수 있으며 이러한 시스템 이벤트들과 이벤트에 대한 로그 생성 시 표현되어야 할 콘텐츠를 정리하면 표 6과 같다.

시스템 이벤트에 대한 로그 정보 또한 시간정보가 기본적인 콘텐츠로 존재해야 하며 이벤트를 구분할 수 있는 행위정보와 필요 시 이러한 행위를 수행하게 된 근거를 표현할 필요가 있다. 이러한 시스템 이벤트 로그들은 시스템에 발생된 문제들을 발견하고 대응하는데 중요한 정보를 제공할 수 있으며 스마트 미터의 시스템 상태를 파악하는 등에 유용한 정보들이 될 수 있으므로 반드시 로그 기록이 필수로 요구된다.

4.2. 스마트 미터 로그 포맷 및 수집 방안

위 Ⅲ장에서 살펴본 내용과 같이 스마트 미터는 기능적, 경제적 등의 이유로 저장 공간이 일반시스템에 비해

〔표 6〕 시스템 이벤트 로그 생성 콘텐츠

시스템 이벤트	콘텐츠 정보
시스템 부팅 및 종료	시간정보, 행위정보(부팅 or 종료), 행위 근거(상위 시스템 명령, 업데이트 반영 등)
하드웨어 및 소프트웨어 오류 (비정상 작동)	시간정보, 오류정보(LCD or S/W 등), 발생 환경(ex, 부팅 or 운영)
템퍼 공격 탐지	시간정보, 행위정보(템퍼 공격 발생)
시스템 업데이트 (펌웨어 등)	시간정보, 행위정보(업데이트), 행위 근거(상위 시스템 명령, 관리 도구에 의한)
통신 연결 및 해제	시간정보, 행위정보(연결 or 해제), 통신대상
시스템 환경설정 변경 (시간정보 등)	시간정보, 행위정보(설정변경), 행위 근거(상위 시스템 명령, 관리 도구에 의한)
시스템 계정정보 변경	시간정보, 행위정보(계정명 변경 등), 행위 근거(상위 시스템 명령, 관리 도구에 의한)
비상 모드(배터리전원 사용 모드) 전환	시간정보, 행위정보(비상모드 전환), 행위 근거(정전 발생)

충분하지 못하며 로그 데이터 저장에 있어 한계가 있다. 또한 스마트 미터는 모든 가구별로 설치되어 운영되므로 다수의 스마트 미터를 관리해야 할 필요성이 존재한다. 따라서 스마트 미터 저장 공간의 한계 및 다수 시스템에서 생성되는 로그 데이터를 보다 효과적으로 관리하기 위해 중앙에서 통합하여 수집할 수 있는 방법이 요구된다.

로그는 스마트 미터뿐만 아니라 스마트그리드 영역에 존재하는 대부분의 시스템, 네트워크 시스템, 보안관련 시스템에서 생성될 수 있다. 생성되는 로그의 포맷이 기존 다른 시스템들과 상이할 경우 통합적으로 수집하고 분석하는데 어려움이 발생될 수 있다. 따라서 대다수의 시스템들이 사용하는 표준화된 로그 포맷이 요구된다. 또한 스마트 미터에서 생성된 로그를 통합수집관리 시스템으로 전송될 경우 도청되거나 데이터 위·변조 등이 발생될 수 있으며 재전송 공격, 송·수신 부인 등의 보안 위협이 발생될 수 있다. 따라서 전송 시 식별 및 인증, 기밀성, 무결성, 가용성, 부인방지와 같은 보안서비스들이 요구된다.

이와 같은 요구사항을 만족하기 위한 로그 관리 방안으로 Syslog를 이용한 방법이 존재한다. Syslog는 1980년에 Eric Allman이 BSD sendmail 프로젝트를 수행하면서 그 일부로 처음 개발되었으며 2001년에 시스코시스템즈의 C.Lonvick이 BSD Syslog Protocol로 IETF Network Working Group에서 RFC 3164을 제정되어 널리 사용되었다[10]. 2009년 3월에 R.Gerhards에 의해 RFC 5424로 개정되었으며, 현재 라우터, 스위치, 방화벽 등과 같은 대다수의 통신장비와 보안장비, 유닉스와 리눅스 시스템에서 일반화되어 표준 로그 프로토콜로 가장 널리 사용되고 있다[11]. 또한 Syslog는 Syslog 서버를 두어 중앙에서 실시간으로 정보를 수집할 수 있도록 지원하며 로그 데이터의 생성, 저장, 전송 등을 지원할 수 있다. 국내에서는 각 시스템별로 상이한 로그 포맷을 표준화하고자 TTA 표준단체를 통해 최종 2011년 12월 21일 'TTAE.IF-RFC5424'를 제개정하여 Syslog를 국내 표준으로 제정하였다. 따라서 Syslog는 이기종 시스템들과 통합적인 로그 관리를 지원하며 국외뿐만 아니라 국외에서도 표준화되어 스마트 미터 로그 생성 및 수집 방안으로써 적절한 방법으로 판단된다.

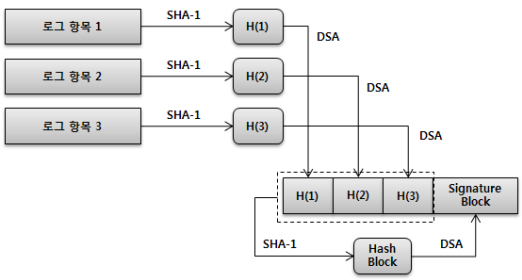
Syslog 구성은 PRI, HEADER, MSG의 세부분으로 나누어 있으며 최대 1024바이트로 구성될 수 있다. PRI 부분은 메시지 분류를 위한 정보이며 우선순위와 중요를 의미하며 헤더부분은 타임스탬프와 호스트명 또는 시스템의 IP주소를 포함하고 있다. 타임스탬프는 Mmm dd hh:mm:ss 형식으로 관리된다. 메시지부분은 실제 생성된 정보를 담는 텍스트 메시지 부분으로 일반적으로 7비트의 아스키 코드로 인코딩된다. syslog 포맷을 이용하여 위에서 식별한 보안감사 이벤트별 메시지 내용의 예를 살펴보면 표 7과 같다.

Syslog 프로토콜은 기본적으로 UDP(User Datagram

〔표 7〕 syslog 기반의 로그 생성 예

이벤트	메시지 내용 예
인증	Feb 2 17:00:50 A-1-Meter(10.10.10.10): Authenticate succeeded from 10.10.10.1 by password manager
요청	Feb 2 17:00:50 A-1-Meter: Requested metering data from 10.10.10.1 success
응답	Feb 2 17:00:50 A-1-Meter: Response metering data to 10.10.10.1 failed - fail access privilege
전달	Feb 2 17:00:50 A-1-Meter: Forwarded bill data from 10.10.10.1 to 10.10.10.2 (IHD-A-1) failed - can't access to network
전송	Feb 2 17:00:50 A-1-Meter: Transported metering data to 10.10.10.2 (IHD) failed - can't access to network
시스템 부팅	Feb 2 17:00:50 A-1-Meter: System booted by remote command from 10.10.10.1
하드웨어 오류	Feb 2 17:00:50 A-1-Meter: Error occur at operation by HW Memory
템퍼 공격 탐지	Feb 2 17:00:50 A-1-Meter: Temper attack attempt!
시스템 업데이트	Feb 2 17:00:50 A-1-Meter: Firmware update from 10.10.10.1
통신 연결	Feb 2 17:00:50 A-1-Meter: Linked ZigBee network with 10.10.10.2 (DCU)
시스템 시간설정 변경	Feb 2 17:00:50 A-1-Meter: Update time information by remote command from 10.10.10.1
시스템 계정정보 변경	Feb 2 17:00:50 A-1-Meter: Modified root password by remote command from 10.10.10.1
비상 모드전환	Feb 2 17:00:50 A-1-Meter: Switch emergency mode by detecting black out

Protocol)을 사용하여 호스트간에 로그들을 전송하여 신뢰성이 보장되지 않는다. 또한 위에서 언급한 식별 및 인증, 기밀성, 무결성, 가용성, 부인방지와 같은 보안서비스를 제공하지 않는다. 따라서 Syslog의 보안성을 높일 수 있는 방법이 요구되며 이를 위해 RFC 5425 "Transport Layer Security (TLS) Transport Mapping for Syslog" 표준을 활용할 수 있다. RFC 5425는 보안 프로토콜로 잘 알려진 TLS를 이용하여 Syslog를 전송하는 방법을 설명하고 있으며 TCP(Transmission Control Protocol) 6154포트를 사용함으로써 UDP 기반의 통신에 비해 전송의 신뢰성을 높일 수 있으며 인증서 기반의 식별 및 상호인증 기능과, 협상된 세션키 및 해시 알고리즘을 통해 기밀성과 무결성을 제공받을 수 있다. 하지만 부인방지 서비스는 TLS를 통해 제공이 불가하며 해당 서비스 제공을 위해 RFC 5848 "Signed Syslog Messages" 방법을 사용할 수 있다[13]. 본 표준은 “syslog-sign”이라 불리며 암호학적으로 서명된 메시지 블록(Signature Blocks)을 그림 4와 같이 사용하여 전송되어야하는 로그 항목에 대해 부인방지 기능을 제공할 수 있다.



〔그림 4〕 서명된 메시지 블록 생성 방법

Ⅴ. 결론 및 향후계획

스마트 미터는 IT기술이 접목되면서 다양한 보안위협에 노출 될 수 있으며 이로 인한 보안 침해사고가 발생 될 수 있다. 무엇보다 스마트 미터는 가정 내에 설치되며 그 수가 많기 때문에 위협원으로 부터 접근이 용이하며 스마트그리드 환경에 존재하는 시스템 중 보안 침해사고가 발생될 가능성이 높다고 할 수 있다. 보안 침해사고를 예방하기 위한 다양한 보안기술들이 개발되고 있지만 그 한계가 존재하며 실제 보안 침해사고를 당했을 경우 그 원인을 파악하고 이를 예방할 수 있는 대책 마련이 중요하다 할 수 있다. 이를 위해 무엇보다 로그 데이터가 중요하며 이를 통해 침입경로 및 새로운 취약점을 발견하는데 핵심적인 자료로 활용될 수 있으며 보안감사 등의 자료로 활용될 수 있다. 하지만 현재로썬 스마트 미터에 요구되는 로그 항목과 스마트 미터 환경을 고려한 로그 관리 방안이 부재하다.

따라서 본 논문에서는 스마트 미터에서 발생될 수 있는 사용사례를 분석함으로써 로그 생성 대상들을 식별하였으며 로그 생성 시 포함되어야할 콘텐츠를 이벤트별로 정리하였다. 스마트 미터 운영환경 특성상 다수의 시스템이 존재하고 로그 데이터를 저장할 만한 충분한 저장 공간이 없으므로 중앙에서 통합적으로 수집할 수 있는 방안이 요구되며 이를 위해 대다수의 네트워크 장치 및 운영체제에서 사용되는 표준 프로토콜인 Syslog 방법을 제시하였다. 하지만 Syslog 프로토콜 자체만으로는 신뢰성 및 보안기능을 제공하지 않으므로 TLS를 이용하여 전송하는 방법과 syslog-sign 방법을 추가로 제시하였다.

본 방안을 통해 스마트 미터 개발 시 로그와 관련된 보안요구사항을 만족할 수 있도록 참고자료가 될 수 있을 것으로 판단되며 스마트 미터에 발생될 수 있는 침해사고를 보다 효과적으로 대응할 수 있을 것으로 기대된다. 추후에는 본 논물을 통해 제시된 방법을 실제 환경에 적용 또는 시뮬레이션 등을 수행해봄으로써 스마트 미터에서 생성되는 로그 생성량을 기초로 요구되는 마이크로프로세서, 휘발성 및 비휘발성 메모리 용량 등을 판단해볼 필요가 있으며 제시된 방법이 실제 해당 환경에 적합한지 실험을 통한 검증이 필요할 것으로 판단된다. 또한 이러한 실험 결과 정보를 바탕으로 보다 스마트 미터 환경에 적합한 로그 관리 방법에 대해 연구할 계획이다.

참 고 문 헌

[1] 전환수, 하영욱, 조병선, “주요 국가의 스마트그리드 정책 동향”, 전자통신동향분석 제25권 제3호, 2010년 6월.

[2] 장두석, “스마트그리드 산업의 동향 및 산업화 방안”, KDBRI, 2010년 1월.

[3] "[특집]보안, 스마트그리드 열기에 불을 지피다-security", 보안뉴스, 2010.08, http://www.boannews.com/media/view.asp?idx=22566&kind=1

[4] “OActive’ Mike Davis to Unveil Smart Grid Research at Black Hat USA,” IOActive press release, 2009.07 http://www.ioactive.com/news-events/DavisSmartGridBlackHatPR.php
[5] SANS, “SANS Eight Annual 2012 Log and Event Management Survey Results”, A SANS Whitepaper, http://www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012-log-event-management-survey-results-sorting-noise-35230
[6] 김완집, 염흥열, "이기종 로그에 대한 통합관리와 IT 컴플라이언스 준수", 한국정보보호학회지 제2권 5호, 2010년 10월.
[7] NIST, "Guidelines for Smart Grid Cyber Security", NISTIT 7628 R1, Oct. 2013.
[8] Advanced Security Acceleration Project (ASAP-SG), "Security Profile For Advanced Metering Infrastructure", osgug.ucaiug.org, Nov. 2009.
[9] freescale, "Smart Grid and Metering Secure end-to-end solutions", http://www.freescale.co.jp/doc/BRSMRTENERGY_rev1.pdf.
[10] RFC 3164, "The BSD Syslog Protocol", IETF Working Group, Aug. 2001.
[11] RFC 5424, "The Syslog Protocol", IETF Working Group, Mar. 2009.
[12] RFC 5425, "Transport Layer Security (TLS) Transport Mapping for Syslog", IETF Working Group, Mar. 2009.
[13] RFC 5848, "Signed Syslog Messages", ETF Working Group, Mar. 2010.
[14] “Guide to Computer Security Log Management", NIST SP 800-92, Sep. 2006., http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf.

〈저자소개〉

사 진

강 성 구(Kang SeongKu)
정회원

2008년 2월 : 충남대학교 컴퓨터공학과 졸업
2011년 2월 : 충남대학교 컴퓨터 공학과 석사
2010년 2월~2011년 2월 : 한국인터넷진흥원 주입연구원
2011년 3월~현재 : ETRI 부설연구소 연구원
관심분야 : 스마트그리드 보안, 디지털포렌식, 네트워크 보안, 정보보호

사 진

김 신 규 (Kim Sinkyu)
정회원

2000년 2월 : 연세대학교 기계전자공학부 졸업
2002년 2월 : 연세대학교 컴퓨터과학과 석사
2014년 2월 : 연세대학교 컴퓨터과학과 박사
2003년 12월~현재 : ETRI 부설연구소 선임연구원
관심분야 : 스마트그리드 보안, 국가기반시설 보안, 취약점 분석