Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.5, October 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.5.873

스마트그리드 제어시스템 보안 위협 평가 방안 연구

고 종 빈,[1†] 이 석 준,[1] 손 태 식[2‡]
[1]아주대학교 컴퓨터공학과, [2]아주대학교 정보컴퓨터공학부

Security Threat Evaluation for Smartgrid Control System

Jongbin Ko,[1†] Seokjun Lee,[1] Taeshik Shon[2‡]
[1]Division of Computer Engineering, Ajou University
[2]Division of Information Computer Engineering, Ajou University

요 약

보안 위협 평가는 시스템의 잠재적인 취약성을 파악하고, 그 취약성 및 대응방안에 대해 객관적인 점수를 부여하는 기술이다. 스마트그리드는 구조적 특성으로 인해 기존의 보안 위협 평가를 적용하기에 무리가 따른다. 본 논문에서는 스마트그리드의 보안 위협 평가를 위해 AMI에 대해 네트워크 모델을 제안하고 공격 시나리오를 도출하였다. 그리고 MTTC scheme을 이용하여 제안 네트워크 모델 및 공격 시나리오에 대해 보안 위협 평가 수행이 가능함을 보였다.

ABSTRACT

Security vulnerability quantification is the method that identify potential vulnerabilities by scoring vulnerabilities themselves and their countermeasures. However, due to the structural feature of smart grid system, it is difficult to apply existing security threat evaluation schemes. In this paper, we propose a network model to evaluate smartgrid security threat for AMI and derive attack scenarios. Additionally, we show that the result of security threat evaluation for proposed network model and attack scenario by applying MTTC scheme.

Keywords: Smartgrid, Security Threat Evaluation, CVSS, MTTC, AMI

I. 서 론

스마트그리드는 기존의 단방향 전력망에 정보통신 기술을 접목하여 실시간으로 전력관련 정보를 주고받음으로써 에너지 효율을 최대화 할 수 있는 차세대 전력망이다. 스마트그리드는 기존 전력망 SCADA(Supervisory Control And Data Acquisition) 시스템의 중앙 연계식 통신 방식을 1:N 방식의 직접 연결로 변화시키고, 이더넷(Ethernet), TCP/IP 등의 보편적인 컴퓨터 통신 프로토콜 및 WLAN, Zigbee 등의 무선 통신 기술을 적극 수용함으로써 스마트그리드 제어 센터와 스마트그리드를 구성하는 수많은 구성요소들과도 유기적으로 데이터를 주고받는 것이 가능하다. 이러한 통신 기술의 진보로 인해 기존의 SCADA 시스템에 비해 편의성과 확장성 측면에서 많은 가능성을 부여하며, 이를 응용한 원격제어, 자동 수요예측 및 반응 등 신기술의 개발 및 적용이 가능하게 되었다. 이처럼 통신 기술의 적용을 통한 많은 이점이 있는 반면에 사이버 보안 측면에서 많은 취약점이 발생할 것으로 예상된다. 그동안의 전력망 SCADA 시스템의 사이버 보안 패러다임은 외부와 독립되고 단절된 형태를 취하는 것이 핵심적인 요소였으나, 스마트그리드 제어시스템은 외부의 네트워크와 다양한 경로를 통해 상호 연결되는 형태를 취함으로써

접수일(2013년 2월 20일), 수정일(1차: 2013년 7월 19일, 2차: 2013년 9월 12일), 게재확정일(2013년 9월 26일)
† 주저자, Jongbin.Ko@gmail.com
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

새로운 관점에서 사이버 보안에 대해 고려할 필요가 있다. 또한, 일반적인 사이버 공격의 대상들과는 달리, 스마트그리드 제어시스템에 대한 공격 발생 시 국가차원의 막대한 피해가 예상되므로 다양한 사이버 보안 위협 및 문제점들을 파악하여 적절한 보안 대책을 수립하고, 시스템에 적용된 보안성의 정도를 평가하여 사이버 공격 발생 시 피해를 최소화할 수 있어야 한다.

스마트그리드 제어시스템의 사이버 공격에 대한 보안성 향상을 위한 선결사항은 스마트그리드를 구성하는 각 시스템 및 네트워크에 대한 보안 취약점을 정확히 파악하는 것이 될 것이다. 보안 위협 평가는 이를 위한 가장 적절한 대안 중 하나이다. 보안 위협 평가는 시스템의 잠재적인 취약성을 파악하고, 그 취약성 및 대응방안에 대해 점수를 부여하여 '얼마나 취약한가?'에 대한 객관적인 지표를 만드는 것을 의미한다. 보안 위협 평가는 일반적인 취약점 분석이 각 장비의 취약점에 대한 설명 및 이를 제거하는 방법을 기술하던 것에 비해 해당 시스템의 전체적인 안전도를 객관적으로 보여줄 수 있다. 따라서 시스템의 전체적인 보안성을 향상 시키고, 보안사고 발생 시 유연한 대처를 가능케 하여 시스템의 보안 수준을 견고한 상태로 유지하는데 기여할 수 있다.

스마트그리드 제어시스템에 대해 보안 위협 평가를 수행하는 것은 여러 가지 어려움이 존재한다. 스마트그리드의 네트워크는 구성 요소에 대한 제어 및 자동화를 위해 상이한 전력기기 간 메시지 교환 표준화가 주 목적이므로, 구조와 특성 면에서 일반적인 컴퓨터 네트워크와 상당이 다른 특징을 나타낸다. 또한, 스마트그리드의 네트워크 말단 디바이스의 대부분은 IED(Intelligent Electronic Devices) 형태로 일반 표준 컴퓨터와 기술적, 성능적으로 큰 차이가 있고, 각 기기간의 연결 형태가 매우 다양하며 그 규모도 상당히 크다. 따라서, 기존의 컴퓨터 네트워크를 대상으로 하는 보안 위협 평가 기법의 적용은 부적절하며, 스마트그리드 제어시스템의 특성에 맞는 네트워크 모델 수립과 공격 경로에 대한 파악이 필요하다.

본 논문의 2장에서는 스마트그리드의 보안 표준들에 대해 알아보고 보안 위협 평가에 대해 논한다. 3장에서는 스마트그리드를 위한 보안 위협 평가 방안으로 스마트그리드를 구성하는 여러 도메인 중 보안 위협 평가의 대상이 될 수 있는 네트워크를 식별하고, 그 중 대표적이라 할 수 있는 AMI에 대한 보안 위협 평가를 위한 네트워크 모델링 어프로치를 제안한다. 4장에서는 제안한 네트워크 모델을 기반으로 공격 시나리오를 제안한다. 5장에서는 제안한 네트워크 모델과 공격 시나리오를 바탕으로 MTTC[1]를 적용하여 수행한 보안 위협 평가 실험 결과를 보인다. 마지막으로 결론 및 향후 연구방향에 대해 논한다.

II. 스마트그리드의 보안 표준 기술 동향

스마트그리드는 정보 통신 기술을 적용하여 상호 통신 및 제어 등 여러 장점을 얻게 되었다. 하지만, 기존 정보 통신망이 지닌 보안 취약점을 그대로 계승하며, Stuxnet[2], Duqu[3], Flame[4]과 같이 SCADA 시스템만을 목표로 하는 악성코드도 점점 늘어가는 추세여서 보안 문제는 스마트그리드의 실용화를 위해 선결되어야 할 시급한 과제라 할 수 있다. 본 장에서는 이와 같은 스마트그리드의 보안 문제점을 해결하기 위해 진행되고 있는 다양한 스마트그리드 보안 표준에 대해 알아본다.

2.1 IEC 62351

IEC(International Electrotechnical Commission) TC57 WG15에서는 IEC SG3이 제시한 스마트그리드 표준화 로드맵을 바탕으로 한 IEC 62351[5] 표준을 제정 및 배포하고 있다.

IEC 62351은 스마트그리드 전력시스템 관리 및 데이터 통신에 대한 보안 기술에 대한 표준으로 초기에는 스마트그리드 내부 통신만을 고려했으나, 연구가 거듭됨에 따라 스마트그리드 전체를 아우르는 보안 표준으로 자리 잡고 있다.

IEC TC57 WG 15에서는 현재까지 IEC 62351 Part 1~8까지의 문서를 발표하였으며, Part 9~11의 표준화를 진행 중이다. 각 파트에서 다루고 있는 내용은 [표 1]과 같다.

2.2 NIST Interagency Report 7628

NIST(National Institute of Standards and Technology)에서는 Interagency Report 7628 for Smart Grid Cyber Security: Guidelines for Smart Grid Cyber Security[6]를 통해 사이버 보안 위험 관리 프레임 워크 및 전략, 개인정보보호 및 스마트그리드, 논리 인터페이스 분석 및 AMI 보안 요구사항을 기술하고 있으며, 스마트그리드의 보안 요구사항에 대한 분석이 포함되어 있다.

〔표 1〕 IEC 62351 Part 별 주제

Part	Topics
1	Introduction
2	Glossary of Terms
3	Data and Communication Security - Profiles Including TCP IP
4	Data and Communication Security - Profile Including MMS
5	Data and Communication Security - Security for IEC 60870 and Derivative (i.e. DNP3)
6	Data and Communication Security - Security for IEC 61850 Peer-to-Peer Profiles
7	End-to-End Security Requirements - Security through Network and System management
8	End-to-End Security Requirements - Role-based Access Control for Power System management
9	End-to-End Security Requirements - Key Management
10	End-to-End Security Requirements - Security Architecture
11	End-to-End Security Requirements - Security for XML Files

2.3 NIST Special Publication 1108

NIST는 2012년 발표한 SP 1108 NIST Framework and Roadmap for Smar Grid Interoperability Standards 2.0[7]에서 스마트그리드 내 구성장치와 시스템 간 상호운용성 및 스마트그리드 환경에서 발생할 수 있는 사이버 보안에 대한 위협 관리 프레임워크 및 전략을 제시하여 1)스마트그리드와 네트워크 도메인의 구조를 설계하기 위한 개념적 참조 모델, 2) 스마트그리드를 위한 75종의 표준, 3) 스마트그리드 내 구성 요소 간 상호운용성 및 신뢰성을 포함한 보안을 위한 추가 표준 재정과 기존 표준에 대한 교정 방안, 4)위기관리 프로세스를 통한 스마트그리드 사이버 보안 전략 및 요구사항 정립, 그리고 5) 스마트그리드 관련 전문가로 구성된 표준 기관에 의해 제출되어야할 행동 계획과 같은 다섯 가지 단계를 제공하고 있다.

2.4 IEC 61850 & GB/T22239

IEC 61850[8]과 GB/T22239[9] 두 표준은 변전소 보호에 관한 기술을 분류하고 있다.

IEC 61850은 IEC 61850-1에서 IEC 61850-9까지로 구성된 변전소 자동화 표준이다. IEC 61850은 데이터 모델링, 보고체계, 이벤트의 고속 전송, 그룹 설정, 샘플 데이터 전송, 명령, 그리고 데이터 저장 매체에 관한 기능명세에 대해 정의하고 있다.

중국의 StateGrid 조합은 GT/T22239: Information security technology-Baseline for classified protection of information system을 중국 국가 표준으로 사용하였는데, 이는 고전압 변전소에 장비의 비용과 위험을 줄이는데 기여했다.

2.5 ITU-T SG17

ITU-T(International Telecommunications Union - Telecommunication Standardization Sector) 내 스마트그리드 보안 분야를 맡고 있는 SG17에서는 스마트그리드 내 홈 영역(Home area)에서 활용될 수 있는 네트워크 보안 표준으로 X.1111 ~ X.1114(홈 네트워크 보안 기술 프레임워크, 홈 네트워크 디바이스 인증서 프로파일, 홈 네트워크 서비스를 위한 사용자 인증 메커니즘 가이드라인, 홈 네트워크 인가 프레임워크)를 개발했으며, 스마트그리드 서비스 구간에서의 보안 위협, 보안 요구사항, 그리고 보안 기능 구조에 대한 표준화를 진행하고 있다.

본 장에서는 스마트그리드의 보안성 향상을 위한 보안 표준들에 대해 알아보았다. 이러한 표준들을 기준으로 많은 보안 기술들이 개발/적용되게 된다. 스마트그리드 제어시스템의 경우 새로운 보안 기술의 개발 및 적용도 중요하지만, 구축된 시스템에 대한 보안 위협을 평가하여 부족한 부분에 대한 신속한 대책 수립을 가능케 할 필요가 있다. 이러한 보안 위협에 대한 평가 부분은 위에서 살펴본 스마트그리드 보안 표준에서는 찾아볼 수 없었으며 ISO/IEC 15408 표준은 보안 등급을 표현하기 위한 것이므로 시스템의 보안 위협에 대해 객관적인 수치로 표현하는 보안 위협 평가와는 방향이 다르다.

III. 스마트그리드 제어시스템 보안 위협 평가 방안

스마트그리드 제어시스템은 구조와 특성이 일반적인 컴퓨터 네트워크와 상이한 특징을 갖고 있다. 스마트그리드 제어시스템의 최상위단 SCADA 시스템 간의 통신은 TCP/IP와 ICCP(Inter-Control Center

Communications Protocol)을 통해 이루어지지만, 하위 제어시스템의 RTU(Remote Terminal Unit) 간 통신을 위해 쓰이는 Serial 기반의 DNP3, IED 간의 통신을 위해 쓰이는 GOOSE, AMI의 스마트 미터링 데이터 교환을 위한 Zigbee 등 특화된 프로토콜을 통해 제어메시지를 주고받게 된다. 또한 스마트그리드 제어 네트워크를 구성하는 대부분의 디바이스들은 하드웨어 적으로도 일반 컴퓨터들과는 상이하다. 이러한 특징들로 인해 기존의 보안 위협 평가 방안들을 적용하는데 많은 어려움이 따른다. 또한, 스마트그리드 제어 네트워크의 대부분은 정확히 동일한 작업을 수행하는 수 없이 많은 동일 디바이스들로 구성되므로, 보안 위협 평가 수행은 동일한 결과가 예상되는 동일한 작업을 수없이 반복해야 하는 비효율성을 지니므로 개선이 필요하다. 따라서 스마트그리드 제어시스템에 대해 효율적이고 정확한 보안 위협 평가를 위해서는 적합한 네트워크 모델링이 선결되어야 한다. 본 장에서는 기존의 보안 취약정 정량화 기법들을 분석한 결과와 스마트그리드 제어시스템 적용의 비 적합성을 논한다. 또한 스마트그리드를 이루는 다양한 네트워크의 보안 위협 평가를 위하여, 2장에서 식별한 구성 요소 중 AMI에 대한 네트워크 모델링 어프로치를 제안한다.

3.1 기존 보안 정량화 기법 분석

3.1.1 CVSS

CVSS(Common Vulnerability Scoring System)[10][11]는 소프트웨어 취약점의 심각한 정도를 국제 공통 기준으로 수치화하기 위해 고안된 산업 표준(de facto standard)이다. CVSS는 복잡한 시스템 환경에서 취약성 평가를 하는데 있어 객관적이고 형식화된 절차를 제공하며, 이 때 사용되는 입력 변수들과 미리 결정된 수치 값들은 체계적으로 분류되어 있다. 또한, 이러한 취약성 평가 절차에 대한 공식 문서는 공개되어 있기 때문에 투명성을 보장한다.

CVSS는 기본적으로 3개의 metric(Base metric, temporal metric, environmental metric)으로 구성되며, 각 metric의 세부내용은 다음과 같다.

• Base metric

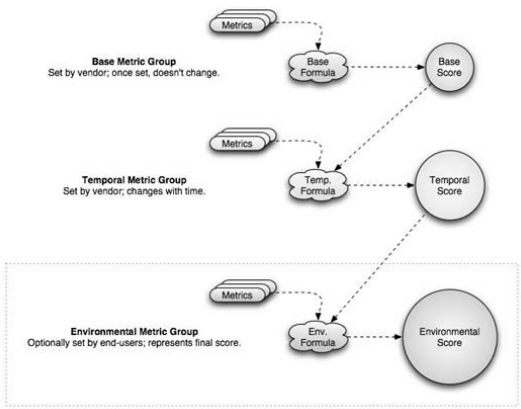
시간과 사용자들에 의해 변하지 않는 취약점의 본질적이고 근본적인 취약점을 다룸. 공격자와 호스트의 거리, 공격 접근 방법의 복잡성 등.

• Temporal metric

사용자들의 환경에 의한 것이 아닌 시간의 흐름에 따라 변경되는 취약점의 특징을 나타냄. 공격 기술이나 코드의 공개 여부, 취약점의 패치 존재 여부 등.

• Environmental metric

공격 성공 시 예상할 수 있는 피해의 규모를 나타냄. 옵션으로 사용되므로 점수에 영향을 주지 않는 개별적인 메트릭스 값 사용



[그림 1] CVSS Metric과 계산 방법[10]

위의 [그림 1]과 같이 base metric을 통해 계산된 base score는 temporal metric의 입력값으로 사용되어 temporal score가 계산되며, 필요할 경우 environmental metric을 이용하여 최종적으로 CVSS 점수를 계산한다. CVSS 점수는 0부터 10 사이에서 부여되며, 10에 가까울수록 취약점의 심각도가 높음을 의미한다.

3.1.2 CVSS의 한계

CVSS는 취약성 점수화를 위해 CVE(Common Vulnerabilities and Exposures)[12], NVD(National Vulnerability Database)[13] 등의 취약점 데이터베이스를 필히 참조해야 한다. 따라서 해당 데이터베이스 내에 적용 근거가 존재 하지 않는다면 CVSS를 통해 취약점을 정량화 하는데 많은 어려움이 따른다. 하지만 보안 취약성은 고정되어 있는 것이 아니며, 기술의 발전과 환경의 변화에 따라 새로운 취약성은 언제든지 발생할 수 있으므로 데이터베이스에 의존하는 CVSS의 취약성 계산 방식은 새로운 취약성에 원활하게 대처하기 힘든 단점이 있다.

또한 스마트그리드 제어시스템은 일반적인 PC 기반의 네트워크와는 통용되는 데이터, 하드웨어의 기능적 차이, 프로토콜의 상이함 등 많은 차이점이 있어 CVSS를 적용하는 것에는 무리가 따른다.

3.1.3 SCADA 보안 취약성 정량화 기법

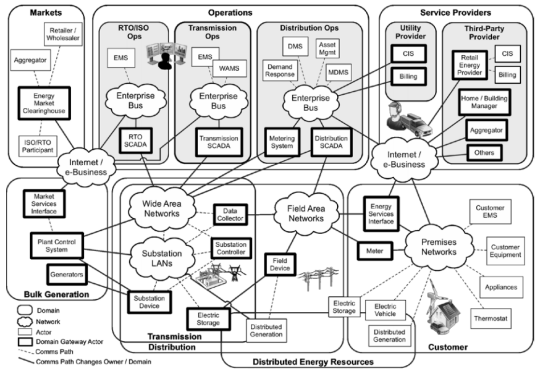
최근의 많은 연구가 보안 취약성 정량화의 대상으로 SCADA 시스템을 지목하였다. 몇몇 논문은 CVSS 혹은 CVSS의 개량화 버전을 SCADA 시스템에 적용하는 시도를 하였다[14][15]. 이러한 아이디어들은 위에서 언급한 CVSS의 본질적인 문제점을 여전히 내포한다. 또한 몇몇 논문은 attack tree와 attack graph를 응용하여 전력 SCADA 시스템에 대한 새로운 보안 취약성 정량화 기법을 제안하였다[16][17]. 일반적으로 스마트그리드와 같은 SCADA 시스템은 광범위한 네트워크에 대해 동작하게 된다. 이 때 수많은 하위 디바이스들이 복잡하고 정교한 네트워크를 구성하게 되므로, 정량화를 위해 모든 케이스에 대해 attack tree 혹은 attack graph를 만드는 것은 상당한 노력이 필요하다.

3.2 보안 위협 평가 대상 네트워크 식별

보안 위협 평가 수행 시 정확하고 면밀한 결과를 얻기 위해서는 대상 시스템의 모든 구성 요소에 대해 보안 취약점을 진단할 필요가 있다. 하지만, 스마트그리드와 같이 국가 단위의 거대한 네트워크의 모든 구성 요소에 대해 보안 취약성을 판단하고 이를 종합하여 보안 위협 평가를 수행하는 것은 매우 어려운 일이다. 또한, [그림 2]과 같이 스마트그리드는 다수 / 이종의 네트워크가 상호 연결된 일종의 국가단위 메쉬 네트워크라 할 수 있으며, 중앙 제어시스템과 각 도메인의 분산 제어시스템이 상호 통신하며 유기적으로 운영된다.

이와 같은 이유로 전체적인 관점에서 스마트그리드의 보안 위협을 평가하는 것은 매우 어려운 일이며, 각 세부 요소별 보안 취약점을 파악하고 이를 종합하여 전반적인 보안 취약사항을 파악하는 것이 바람직하다. 또한, 각 구성 요소가 상호 연결되었을 때 새롭게 발생할 수 있는 취약점을 고려하여 전체적 보안 위협 평가를 수행하여야 한다.

스마트그리드는 기존 전력망의 구성 요소와 새롭게 추가된 구성 요소가 혼재한다. 이러한 스마트그리드의 구성 요소 중 발전소 등과 같이 일반인의 접근이 여전히 어려운 요소들은 상대적으로 외부로부터의 공격에 덜 취약할 것이다. 반대로 새롭게 추가된 요소 중 모든 가정에 설치되는 스마트 미터 등은 상대적으로 공격에 취약하다. 따라서 다른 요소들에 비해 공격에 노출되기 쉽거나, 노출되었을 시 치명적일 수 있는 부분에 대해 우선적으로 보안 취약성을 파악할 필요가 있다. 보안 위협도가 높은 것으로 예상되는 스마트그리드의 도메인은 AMI(Advanced Metering Infrastructure), 자동화 변전소(automated substation), 전기 자동차 및 충전 인프라, 마이크로그리드(microgrid) 등이다.



[그림 2] 스마트그리드 네트워크 아키텍쳐[7]

특히 AMI의 경우 스마트 미터가 기존 전력 검침기를 대체하여 모든 세대에 설치되게 되므로 공격자가 검침 정보 조작 등을 위해 손쉽게 접근이 가능하다. 또한, 데이터가 집중되는 DCU가 공격에 노출되면 심각한 피해를 입힐 수 있으므로 철저한 대비가 필요하다. 따라서, 본 논문에서는 스마트그리드 제어시스템의 도메인 중 AMI를 보안 위협 평가 대상으로 선정하여 네트워크 모델링을 진행하였다.

3.3 레벨(level)과 디바이스 그룹화

- 레벨 기반 네트워크 모델링

첫 번째로 대상 네트워크의 구성 요소별 데이터 민감도에 따라 영역을 구분을 할 필요가 있다. 일반적으로 제어시스템 네트워크는 계층적 구조를 가지고 있으며, 각 계층별로 생산하는 데이터에 대한 민감도가 다르다. 따라서 비슷한 민감도를 지닌 계층을 하나의 영역으로 묶고 이것을 레벨이라 칭한다. 이러한 레벨화는 대상 네트워크에서 보호해야 할 대상의 우선순위를 정할 수 있으며, 상대적으로 보호가 불필요 하거나 공격자가 공격을 위해 접근하기 매우 어려운 경우 취약

성 정량화 대상에서 제외함으로써 효율성을 높일 수 있다.

본 논문에서는 AMI의 DCU와 스마트미터를 'Consumer level', AMI head end와 mangement console을 'AMI head end level'로 각각 정의하였다. 또한 DMS, OMS, MDMS 등의 제어 부를 'Control center level'로 정의하였다.

• 디바이스 그룹화

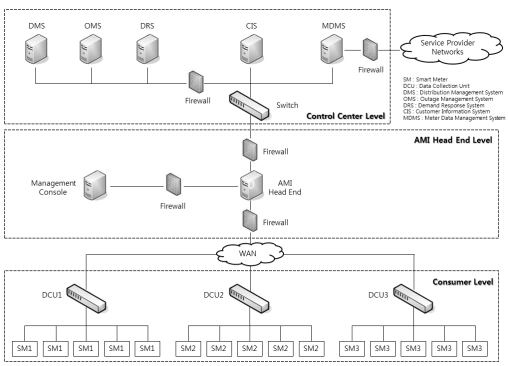
제어시스템 네트워크는 스마트그리드 구성 디바이스(DCU, IED, 스마트미터 등) 뿐 만 아니라, 일반 네트워크 디바이스인 스위치(switch), 파이어월(firewall) 등 다양한 네트워크 디바이스가 통합된 환경으로 구축된다. 이러한 통합 환경의 보안 위협 평가를 위해 디바이스들의 특성에 따른 그룹화가 필요하다. 이러한 그룹화는 앞서 설명한 동일한 작업을 최대한 배제하여 작업의 효율성을 높이고, 네트워크 구조에 대한 이해도를 높여 공격 경로 예측 등에 도움을 줄 수 있다.

각 그룹은 동일한 작업을 수행하는 디바이스 별로 그룹화 되고, 동일 그룹 내에서 제조사 특성에 따라 재 구분된다. 그 후 그 외의 네트워크 기기들이 특성별로 그룹화 된다.

AMI의 수많은 스마트미터가 동일한 작업을 수행하나, 일정 수의 스마트미터는 특정 DCU로 데이터를 집중하므로 DCU를 기준으로 그룹화를 수행하였다. 각 DCU의 스마트미터들은 하나의 그룹을 형성하므로 보안 위협 평가 시 하나의 개체로 인식되어 평가된다.

3.4 제안하는 AMI 네트워크 모델링 어프로치

〔그림 3〕은 제안하는 AMI의 보안 위협 평가를 위한 네트워크 모델이다. 기능에 따라 Control center level, AMI head end level, Consumer level로 구분하였으며, Consumer level의 스마트미터들은 DCU를 기준으로 그룹화가 적용되었다.



〔그림 3〕 보안 위협 평가를 위한 AMI 네트워크 모델링

IV. 보안 취약성 검증을 위한 공격 시나리오

4.1 네트워크 존(zone) 구분

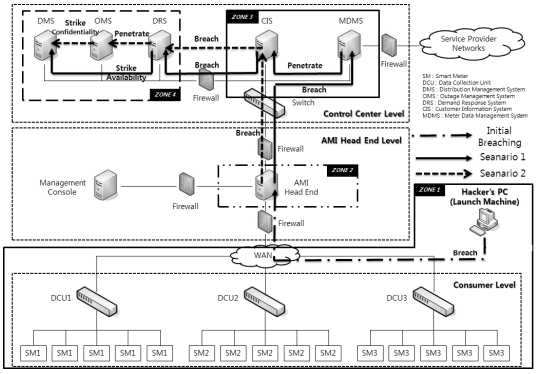
우선 공격 시나리오를 설정하기 위하여, 네트워크 모델을 방화벽 기준으로 구분하여 존(zone)을 설정하였다. 우선 공격자의 PC가 포함되어 공격이 시작되는 지역을 'Zone 1'로써 하나의 존으로 설정하고, 두 번째로 AMI head end 장비가 포함된 존을 'Zone 2'로 설정하였고, Control center level에서 CIS와 MDMS가 존재하는 지역을 'Zone 3'로 설정하고 마지막으로 DMS, OMS, DRS가 설치된 지역을 'Zone 4'로 설정했다. 이렇게 방화벽을 기준으로 Zone을 설정하는 이유는, 방화벽과 같은 보안 장비를 통과해야 하는 공격과, 보안장비를 거치지 않는 공격은 유형이 다르기 때문이다.

따라서 공격유형은 크게 두 가지로 볼 수 있다. 한 존에서 다른 존의 장비로의 공격이 있으며, 이를 Breach라 하고, 한 존 내에서 다른 장비로의 공격은 Penetrate라 한다. 이때의 공격은 대상 장비의 관리자 권한을 얻거나 감염시켜, 그를 이용해 다시 공격을 재개할 수 있는 수준의 공격을 말한다.

4.2 공격 시나리오

공격 시나리오는 다음과 같다. 공격자의 컴퓨터는 〔그림 4〕에서 'Zone 1'에 있으며, 최종 공격(compromise)대상은 'Zone 4'의 최 좌측 상단에 위치하는 DMS이다. 공격은 Zone 단위로 수행되며, 'Zone 1'로부터 'Zone 2', 'Zone 3'을 거쳐 'Zone 4'의 DMS를 공격하게 된다. 공격자는 내부로의 초기 침투 과정으로 'Zone 2'에 위치하는 AMI head end의 취약점을 이용하여 'Zone 2'에 침투(Breach)한다.

AMI head end로 침투한 이후에는 두 가지 경로로 DMS에 공격을 하게 된다. 첫 번째 경로는 'Zone 3'의 MDMS의 제어권을 얻고 같은 Zone 내의 CIS로 침투하여 'Zone 4'의 DRS를 거쳐 DMS에 가용성을 해치는 공격을 수행하는 것이고, 두 번째 경로는 'Zone 2'에서 'Zone 3'의 CIS를 바로 침투해 'Zone 4'의 DRS, OMS를 거쳐 DMS의 기밀성을



〔그림 4〕 제안하는 네트워크 모델에 대한 공격 시나리오

해치는 공격을 수행하는 것이다.

본 논문에서는 공격자로부터 공격 시나리오를 설정하기 위해 위와 같이 설명하였으나, 'Zone 1'에서 공격을 시작하지 않아도, 'Zone 2'의 감염된 컴퓨터, 혹은 악의 목적의 내부 사용자가 'Zone 3', 'Zone 4' 내부의 장비들을 직접적으로 공격할 수도 있다.

V. 제안 모델 검증

제안한 네트워크 모델과 이를 대상으로 한 공격 시나리오에 따라 보안 위협 평가를 수행한 결과를 수록한다. 보안 취약성 정량화를 위한 여러 종류의 기법이 존재하지만 그 중 가장 대표적인 CVSS는 앞서 설명한 것과 같이 적용하는데 여러 문제점이 존재한다. 따라서 본 논문에서는 2008년 D. Leversage 등이 제안한 MTTC〔1〕를 적용하여 제안 모델의 보안 위협 평가를 수행하였다. MTTC는 CVSS와는 달리 보안 위협 평가 결과를 공격 루트에 따라 공격 성공에 걸리는 시간으로 표현하여 좀 더 직관적인 정보를 보안 관리자에게 제공할 수 있고, CVE에 대한 의존도가 낮은 장점이 있다.

MTTC는 공격 경로 상에 존재하는 보안 취약점의 개수가 매우 중요한 비중을 차지한다. 보안 취약점의 개수는 여러 가지 방법으로 확인할 수 있다. 특정 시스템의 보안 취약점을 파악하는 방법은 여러 가지가 있지만, MTTC는 단순히 취약점의 개수가 필요하므로 Nessus 등의 보안 취약성 스캐닝 툴을 이용하여 취약성의 개수를 파악하는 것을 가정할 수 있다.

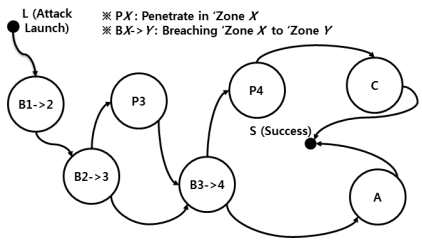
〔표 2〕은 제안하는 네트워크 모델에 대해 Nessus 등의 보안 취약성 스캐닝 툴을 이용하여 얻을 수 있는 보안 취약성의 개수이다.

〔표 2〕 공격 경로에 포함되는 각 장비들의 취약점 개수

대상	취약점 개수(권한 획득 관련)
DMS	2
OMS	3
DRS	3
CIS	4
MDMS	2
AMI Head End	5

5.1 Attack-Graph 설정

〔그림 5〕는 네트워크 모델에서 공격 경로를 파악한 것에 대한 Attack-Path 그래프를 설정한 것이다. Attack Launch(L)부터 Breach(Bx)로 시작하여 기밀성(C), 가용성(A)을 해치면 Attack Sucess(S)까지 도달하는 State를 표현한 그래프이다.



〔그림 5〕 공격 경로에 대한 Attack-Path 그래프

위와 같이 Attack-Graph를 설정하면 공격 경로를 쉽게 파악할 수 있다. 〔그림 5〕에서 도출할 수 있는 공격 경로는 다음의 네 가지이다.

L, B1->2, B2->3, P3, B3->4, P4, C
L, B1->2, B2->3, P3, B3->4, A
L, B1->2, B2->3, B3->4, P4, C
L, B1->2, B2->3, B3->4, A

위 네 가지 공격 경로에 대한 MTTC를 구하기 위해 B1->2, B2->3, B3->4, P3, P4, C(strike Confidentiality), A(strike Availability) 각각에 대해서 TTC를 구하고 L->S의 각 경로에 대한 가중치를 적용하면 MTTC를 계산할 수 있다.

5.2 실험결과

MTTC는 특정 공격 목표에 대한 다수의 공격경로별 각각의 TTC를 구하여 계산한 TTC의 평균값을 의

미한다. 또한 MTTC는 공격대상에 대하여 공격자의 skill level 별로 가중치를 부여하여 계산하므로 좀 더 객관적인 정보를 얻을 수 있다.

제안한 네트워크 모델 및 공격 시나리오에 대한 MTTC 실험 결과를 〔표 3~9〕와 같이 얻을 수 있었다. 먼저 Attack-Graph의 1->2, B2->3, B3->4, P3, P4, C, A에 따른 TTC 값을 구하여야 한다. 이 때, MTTC에서 제안하는 여러 단계가 필요하나, 각 단계에 대한 세부적인 설명은 본 논문의 논지에서 벗어나므로 계산 결과만을 수록한다. 계산을 위해 필요한 각 변수의 설정은 실험을 위해 실제보다 단순하게 정의하였다. Strike Confidentiality와 Strike Availability는 공격자가 제어시스템의 프로토콜이나 데이터 암호화 처리 방식 등을 충분히 이해하고 있다고 가정하여 제어권 획득 후 약 1일이 소요 되는 것으로 설정하였다. 알려진 총 취약점의 개수 K는 NVD(National Vulnerability Database)의 모든 취약점의 개수를 파악하여 50000으로 설정하였다. 사용가능한 Exploit의 개수는 유명 exploit 웹 사이트인 www.metasploit.com에 공지된 정보를 토대로 1800으로 설정하였다. 공격자 실력에 대한 가중치 s는 상급자의 경우 1.0, 중급자는 0.9, 초보자는 0.5로 설정하였으며, 네트워크 관리자가 방화벽을 점검하는 빈도에 대한 가중치 α는 semi-annual(연 2회)에 대한 값 0.3으로 설정했다. V는 공격 대상이 되는 Zone의 취약성 개수의 평균값이다. 다음의 〔표 3~8〕는 공격 시나리오에 따른 TTC 계산 결과이다.

〔표 3〕 Zone 1에서 Zone 2로 Breach 공격 시 TTC

	Expert	Intermediate	Beginner
P1	0.052568	0.047438	0.026639
u	0.000000	0.031623	0.353553
ET	1.000000	0.900000	0.593750
t3	21.010000	24.390000	51.430000
s	1.0	0.9	0.5
V	5.0	5.0	5.0
TTC	5.55	5.60	19.90

〔표 4〕 Zone 2에서 Zone 3로 Breach 공격 시 TTC

	Expert	Intermediate	Beginner
P1	0.031881	0.028739	0.016069
u	0.000000	0.125893	0.535887
ET	1.000000	0.900000	0.250000
t3	21.010000	24.390000	51.430000
s	1.0	0.9	0.5
V	3.0	3.0	3.0
TTC	5.65	7.44	27.80

〔표 5〕 Zone 3 내에서 Penetrate 공격 시 TTC

	Expert	Intermediate	Beginner
P1	0.031881	0.028739	0.016069
u	0.000000	0.125893	0.535887
ET	1.000000	0.900000	0.250000
t3	21.010000	24.390000	51.430000
s	1.0	0.9	0.5
V	3.0	3.0	3.0
TTC	5.65	7.44	27.80

〔표 6〕 Zone 3에서 Zone 4로 Breach 공격 시 TTC

	Expert	Intermediate	Beginner
P1	0.028389	0.025587	0.014297
u	0.000000	0.158489	0.574349
ET	1.000000	0.900000	0.300000
t3	21.010000	24.390000	51.430000
s	1.0	0.9	0.5
V	2.666667	2.666667	2.666667
TTC	5.66	8.07	29.86

〔표 7〕 Zone 4 내에서 Penetrate 공격 시 TTC

	Expert	Intermediate	Beginner
P1	0.028389	0.025587	0.014297
u	0.000000	0.158489	0.574349
ET	1.000000	0.900000	0.300000
t3	21.010000	24.390000	51.430000
s	1.0	0.9	0.5
V	2.666667	2.666667	2.666667
TTC	5.66	8.07	29.86

〔표 8〕는 하나의 공격(Breach, Penetrate) 수행에 따른 TTC 계산 결과이다.

〔표 8〕 State에 따른 TTC 계산 결과 (days)

	Expert	Intermediate	Beginner
B1->2	5.55	5.60	19.90
B2->3	5.65	7.44	27.80
B3->4	5.66	8.07	29.86
P3	5.65	7.44	27.80
P4	5.66	8.07	29.86
SC	1.0	1.0	1.0
SA	1.0	1.0	1.0

*SC : Strike Confidenciality,
SA : Strike Availability

이렇게 계산된 TTC 값을 바탕으로 최종적 보안 취약성 정량화 점수인 MTTC 값을 계산하게 된다. 〔표 9~11〕은 본 논문에서 제안한 제어시스템 네트워크

모델의 공격 시나리오에 대한 최종 MTTC 계산 결과이다.

〔표 9〕 타겟에 대한 상급자의 MTTC 계산

Attack Path	Probability	Path Time	Product
L, B1->2, B2->3, P3, B3->4, P4, C	1/4	29.17	7.2925
L, B1->2, B2->3, P3, B3->4, A	1/4	23.51	5.8775
L, B1->2, B2->3, B3->4, P4, C	1/4	23.52	5.88
L, B1->2, B2->3, B3->4, A	1/4	17.86	4.465
MTTC(Expert)		23.52 days	

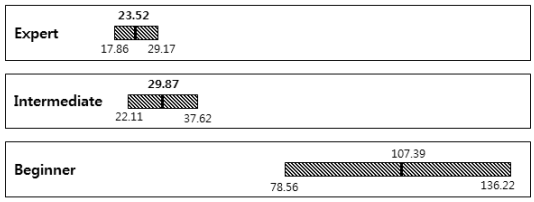
〔표 10〕 타겟에 대한 중급자의 MTTC 계산

Attack Path	Probability	Path Time	Product
L, B1->2, B2->3, P3, B3->4, P4, C	1/4	37.62	9.405
L, B1->2, B2->3, P3, B3->4, A	1/4	29.55	7.3875
L, B1->2, B2->3, B3->4, P4, C	1/4	30.18	7.545
L, B1->2, B2->3, B3->4, A	1/4	22.11	5.5275
MTTC(Intermediate)		29.87 days	

〔표 11〕 타겟에 대한 초급자의 MTTC 계산

Attack Path	Probability	Path Time	Product
L, B1->2, B2->3, P3, B3->4, P4, C	1/4	136.22	34.055
L, B1->2, B2->3, P3, B3->4, A	1/4	106.36	26.59
L, B1->2, B2->3, B3->4, P4, C	1/4	108.42	27.105
L, B1->2, B2->3, B3->4, A	1/4	78.56	19.64
MTTC(Beginner)		107.39 days	

〔그림 6〕은 DMS에 대한 MTTC 계산 결과를 그래프로 표현한 것으로써, MTTC 계산을 위한 TTC의 최소값과 최대값이 표현되므로 MTTC interval 불린다. 가로축은 MTTC 값으로써 공격에 소요되는 일 수(days)를 나타낸다. Expert의 경우 설정된 시나리오의 공격 경로 두 가지에 따라 각각 최소 TTC인 17.86 days와 최대 TTC인 29.17 days가 계산된다. 공격 가능 한 경로별로 계산된 TTC들의 동일한 가중치(1/4)을 적용하면 최종 MTTC 값인 23.52 days가 도출된다. 같은 방식으로 intermediate attacker는 29.87 days, Beginner attacker는 107.39 days가 MTTC 값으로 도출되었다.



〔그림 6〕 MTTC Interval

〔표 9~11〕의 Attack Path는 본 논문에서 설정한 네트워크 모델에서 DMS를 공격하는 두 가지 시나리오에서 도출된 Attack-Graph를 통해 공격 가능한 4가지 경로를 추출한 것이다.

만약 추출한 공격 경로 각각에 있어서, 그 경로 중 한 부분에서 공격당하는 기기와 동일한 기기가 같은 Zone에 존재할 경우, 공격자는 두 기기 중 하나를 선택하면 공격에 성공할 수 있다. 따라서 위와 같은 경우에는 총 공격 경로의 수를 1 증가시키고, 가중치(공격에서 경로가 선택될 확률, Probability)를 증가시키면 쉽게 계산이 가능하다.

본 논문의 모델에서는 위의 조건에 부합하지 않으므로 4개의 경로는 그 각각 경로에 대한 가중치가 1/4씩 주어지고, 각각의 경로에 대해 계산한 TTC 값에 그 가중치를 부여해 MTTC를 계산하였다. 실험결과로부터 본 논문에서 제안하는 네트워크 모델과 공격 시나리오를 이용해 적절한 보안 취약성 정량화가 가능함을 확인할 수 있었다.

VI. 결론

본 논문에서는 스마트그리드 제어시스템의 전체적인 보안 위협 평가를 위해서 스마트그리드 구성 도메인 중 AMI 보안 위협 평가 대상으로 식별하여 정량화 네트워크 모델을 도출하고 공격 시나리오를 구성하였다. 이렇게 도출된 네트워크 모델과 공격시나리오에 대해서 MTTC를 적용하여 보안 위협 평가를 수행하였다. 제안 모델을 검증하기 위하여 실험 데이터는

최종 공격 목표가 DMS일 경우를 가정하여 보안 위협 평가를 수행하였다. 추후 실제 AMI를 비롯한 스마트 그리드 제어 시스템에 대한 전반적인 보안 위협 평가를 수행하기 위해서는 네트워크 내의 사이버 공격이 가능한 모든 장비들에 대해 공격 루트 파악 및 이에 따른 적합한 보안 위협 평가를 수행하고 그 결과들을 종합하여 분석을 수행해야 할 것이다.

참고문헌

〔1〕 D.J. Leversage, and E. James, "Estimating a System's Mean Time-to-Compromise," Security & Privacy, IEEE, vol. 6, no. 1, pp. 52-60, Jan. 2008.

〔2〕 N. Falliere, L.O. Murchu and E. Chien, "W32.Stuxnet Dossier," Symantec sercurity Response, Feb. 2011.

〔3〕 Symantec, "W32.Duqu: The Precursor to the Next Stuxnet Version 1.4," Symantec Security Response, Nov. 2011.

〔4〕 sKyWIper Analysis Team, "sKyWIper (a.k.a Flame a.k.a. Flamer) : A complex malware for targeted attacks," CrySyS Lab, May. 2012.

〔5〕 IEC, "Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines," IEC 62351-10, Oct. 2012.

〔6〕 NIST, "Guidelines for Smart Grid Cyber Security," NISTIR 7628, Aug. 2010.

〔7〕 NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 2.0," NISTSP 1108, Feb. 2012.

〔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〕 Chinese National Standard, "Information security technology-basic requirements of grade protection of information system security," GB/T22239-2008, 2008.

〔10〕 P. Mell, K. Scarfone and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," Forum of Incident Response and Security Teams, Jun. 2007.

〔11〕 박중길, "정보 시스템 취약도 계산 방법 개발," 정보보호학회논문지, 17(5), pp. 131-179, 2007년 10월.

〔12〕 P. Mell, and T. Grance, "Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme," NISTSP 800-51, 2002.

〔13〕 NVD, "US National Vulnerability Database," http://nvd.nist.gov/, Feb. 2011.

〔14〕 M. Hentea, "Improving Security for SCADA Control Systems," Interdisciplinary Journal of Information, Knowledge, and Management, vol. 3, pp. 73-86, 2008.

〔15〕 A. Hahn, "Smart Grid architecture risk optimization through vulnerability scoring," Innovative Technologies for an Efficient and Reliable Electricity Supply (CITRES), 2010 IEEE Conference on, pp.36-41, Sep. 2010.

〔16〕 J.L. Bayuk, and A. Mostashari, "Measuring cyber security in intelligent urban infrastructure systems," Emerging Technologies for a Smarter World (CEWIT), 2011 8th International Conference & Expo on, pp.1-6, Nov. 2011.

〔17〕 Y. Jiaxi, M. Anjia, and G. Zhizhong, "Vulnerability Assessment of Cyber Security in Power Industry," Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES, pp.2200-2205, Oct. 2006.

〈저자소개〉

고 종 빈 (Jongbin Ko) 학생회원
2006년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2008년 2월: 아주대학교 정보통신전문대학원 공학석사
2008년 3월~현재: 아주대학교 컴퓨터공학과 박사과정
〈관심분야〉 스마트그리드 보안, 보안 위협 평가, 전기자동차 보안, 디지털 포렌식

이 석 준 (Seokjun Lee) 학생회원
2011년 8월: 아주대학교 정보 및 컴퓨터공학부 졸업
2011년 9월~현재: 아주대학교 컴퓨터공학과 석사과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 모바일 네트워크 보안

손 태 식 (Taeshik Shon) 종신회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 정보통신전문대학원 공학석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월: Research Scholar, University of Minnesota
2005년 8월~2011년 2월: 삼성전자 DMC 연구소 책임연구원
2011년 3월~현재: 아주대학교 정보통신대학 정보컴퓨터공학과 조교수
〈관심분야〉 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지, ICT융합보안