스마트 그리드에서 사이버 보안 기술 적용을 위한 공통의 공격 트리에 관한 연구

김영곤, 이은규
인천대학교 정보통신공학과
e-mail : eklee@inu.ac.kr

Study on Common Attack Trees in Cybersecurity of Smart Grid

Young Gon Kim and Eun-Kyu Lee
*Dept. of Information and Telecommunication Engineering, Incheon National University

요 약

스마트 그리드는 노후화된 전력망에 정보통신 기술을 융합하여 지능화시킴으로써, 전력 사용을 가능한 효율적으로 만들기 위한 기술이다. 대표적인 융합 기술이기 때문에, 시스템의 보안 취약점이 많아질 수 밖에 없다. 이러한 이유로 보안 기술에 대한 관심이 많아지고 있으며, 개별 어플리케이션 도메인에서 발생할 수 있는 사이버 보안 실패 시나리오에 대한 분석이 활발히 이루어지고 있다. 본 논문에서는 어플리케이션 도메인내 실패 시나리오의 공격 트리를 분석하여 공통적으로 발생하는 있는 8 개의 공격 모델에 대한 공격 트리를 정리하고 이를 도식화한다.

1. 스마트 그리드 개요

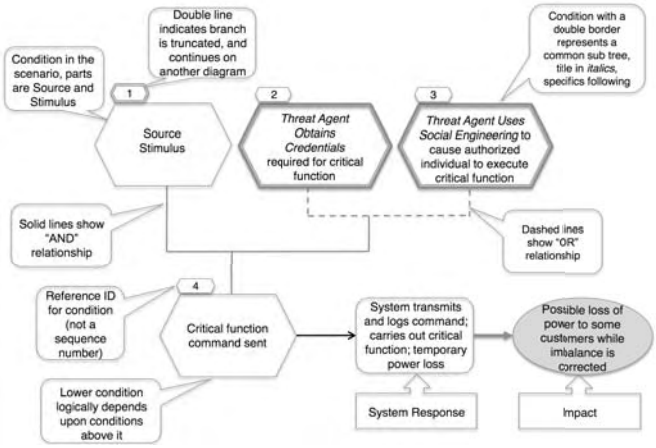
스마트 그리드는 현대 사회 발전의 필수 자원 중에 하나의 전력/전기를 가능한 효율적으로 사용하는 것을 목표로 한다. 이를 위해, 스마트 그리드는 기존의 노후화된 전력망에 정보통신 기술을 접목함으로써, 에너지 관련 장비가 상호 통신을 하고, 지능적으로 동작할 수 있도록 한다. 스마트 그리드는 대표적인 융합 기술이며, 이로 인해 다양한 보안 취약점 보인다. 미국의 표준 기관인 NIST 는 스마트 그리드 보안 기술을 다양한 관점에서 분석하고 필요한 세부기술들을 정리하고 있다 [1]. 이러한 보안 기술들은 아래에 보이는 6 개의 스마트 그리드의 어플리케이션 도메인에 개별적으로 적용될 수 있다 [2].

(A) Advanced Metering Infrastructure (AMI)
(B) Distributed Energy Resources (DER)
(C) Wide Area Monitoring, Protection, and Control (WAMPAC)
(D) Electric Transportation (ET)
(E) Demand Response (DR)
(F) Distribution Grid Management (DGM)

최근의 NESCOR 프로젝트는 개별 도메인에서 보안을 위협하는 실패 시나리오 (failure scenario)를 정리했으며, 해당 시나리오를 예방하기 위한 기술 전략을 제안하고 있다 [4]. 이러한 실패 시나리오는 도식화하여 공격 트리로 표현될 수 있고, 참고 문헌 [5]는 가장 가능성이 높고 취약성이 높은 일부의 실패 시나리오들에 대한 공격 트리를 표시한다. 본 논문에서는 어플리케이션 도메인내 실패 시나리오의 공격 트리를 분석하여 공통적으로 발생하는 있는 8 개의 공격 모델에 대한 공격 트리를 정리하고 이를 도식화한다.

2. 공격 트리

공격 트리는 자산 또는 대상이 공격받을 수 있는 방법을 보여주는 개념 다이어그램이며, 다양한 응용 분야에서 사용되고 있다. 정보 기술 분야에서는 컴퓨터 시스템에 대한 위협과 그러한 위협을 실현하기 위한 가능한 공격을 설명하는데 사용된다. 그러나, 공격 트리의 응용 분야는 전통적인 정보 시스템의 분석에만 국한되지 않는다. 이들은 변조 방지 전자 시스템 (예를 들어, 군용 항공기의 항공 전자 공학)에 대한 위협 분석을 위해 방위 및 우주 항공 분야에서도 널리 사용된다 [3]. 최근에는 스마트 그리드와 같은 사이버-물리 시스템에서 제어 모듈을 적용하는데 활용되고 있다 [6]. 본 논문에서는 스마트 그리드 분야에서 실현 가능한 공격을 설명하기 위해 사용한다.



(그림 1) 공격 트리 다이어그램 해석을 위한 설명[5].

그림 1 에서 보이는 바와 같이 공격 트리는 작은 육각형에 번호가 매겨진 이중선으로 표시된 잘린 가지가 있으며, 이 가지들은 다른 그림에 나타날 수 있다. 각 육각형은 실패 시나리오를 구성하는 일련의 조건에서 개별 조건을 나타낸다. 잎과 직접 연결되어 있는 잎은 그 잎이 생기기 위해 필요한 모든 조건을 표시한다. 조건은 실패 시나리오 내에서 발생하는 몇 가지 단계에 대해 설명할 수 있다. 공격 트리는 발생하는 순서에 따라 위에서 아래로 읽는다. 사실, 표준 공격 트리는 아래에서 위쪽 방향으로 진행하며 해석한다. 스마트 그리드 분야에서의 공격 트리는 가독성의 향상시키기 위해 표준 모델과는 반대로 설계되어 있다. 조건은 해당 조건을 시작한 SOURCE 및 시작된 조치 (STIMULUS)로 표시(라벨링)된다. SOURCE 는 일반적으로 사람이거나 사이버 구성 요소이다. 각 육각형 (조건)을 라벨링하는 숫자는 사용자가 그림의 특성을 참조 할 수 있게 하는 ID 이며, 그들은 상태의 순서를 나타내지는 않는다. 이중 경계는 분기가 절단되어 다른 다이어그램에서 계속됨을 나타낸다.

두 개의 조건을 하나의 선으로 연결하는 것은 우선 순위가 낮은 조건이 높은 조건에 의해 결정된다는 것을 의미한다. 점선의 연결은 "OR" 연산을 의미한다; 즉, 연결된 상위 조건 중 하나 또는 다른 조건이 발생할 경우 낮은 조건이 발생할 수 있다. 낮은 조건이 발생하기 위해 모든 상위 조건이 필요한 경우 실선이 사용되어 "AND" 연산을 의미한다. 공격 트리의 맨 아래에는 두 개의 추가 노드가 있다. 첫 번째 노드는 실패 시나리오가 발생한 후(시스템 응답), 시스템에 어떤 일이 발생 하는지를 나타낸다. 시스템 응답은 둥근 사각형으로 표시되고 두 번째는 타원형으로 표시된다.

3. 공통의 공격 트리

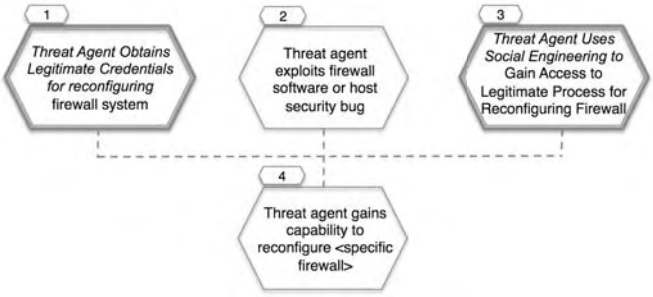
공통의 공격 트리는 여러 공격 트리에서 사용되는 하위 집합을 나타내는 단순화 기법으로, 그림 1 에서는 두 개의 윤곽선이 있는 육각형으로 표시된다. 모듈식 하위 집합을 만드는 것은 공통된 세부 사항을 자신의 트리에 문서화함으로써 특정 공격 트리를 단순화시킬 수 있다. 그런 다음 특정 트리는 참조되는 방식에 대한 관련 컨텍스트와 함께 일반적인 공격 하위 트리를 인스턴스화 한다. 공통의 공격 트리는 "공격자가 유효한 인증 정보를 획득한다"와 같은 일반적인 이름을 가지지만 "시스템 또는 기능"이라는 컨텍스트도 포함할 수 있다. 특정한 공격 트리가 공통의 공격 트리를 참조할 수 있으며, 이 때, 참조하는 "시스템 또는 기능" 정보를 구체화할 수 있다.

NESCOR 실패 시나리오 문서로부터 대표적인 스마트 그리드 도메인에 대한 공격 트리가 도출되었다 [4]. 여러 상황에서 공통 분기가 있는 위치를 이해함으로써 아래와 같은 8 개의 공통의 공격 트리가 완성된다. 공통 분기 위치가 추상화되고 공통의 공격 트리에서 '<>'표기법을 통해 인스턴스화 될 수 있다. 해당 공통 공격 트리가 일반 공격 트리에서 참조될 때, 괄호 안에 적절한 세부 내역이 채워지게 된다.

(A)Threat Agent Gains Capability to Reconfigure <firewall>
(B)Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
(C)Authorized Employee Brings Malware into <system or network>
(D)Threat Agent Obtains Credentials for <system or function>
(E) Threat Agent Uses Social Engineering to <desired outcome>
(F) Threat Agent Exploits Firewall Gap in <specific firewall>
(G)Threat Agent Exfiltrates <data>
(H)Threat Agent Gains Access to <network>

Threat Agent Gains Capability to Reconfigure <firewall>.

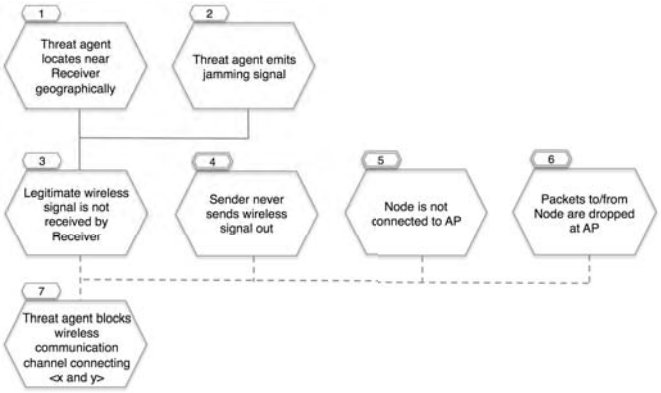
공격자는 특정 방화벽에서 방화벽 규칙을 변경할 수 있는 권한을 획득한다. 이후 방화벽을 통해 특정한 형태의 데이터들이 특별한 제재없이 통행할 수 있도록 함으로써 미래에 사이버 공격을 할 수 있도록 한다. 이러한 위협은 방화벽에 접근할 수 있는 인터페이스가 있으며, 공격자가 네트워크를 통해 여기에 접근할 있다는 것을 가정한다. 그림 2 는 (A) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 2) (A) 위협에 대한 공격 트리 다이어그램.

Threat Agent Blocks Wireless Communication Channel Connecting <x and y>.

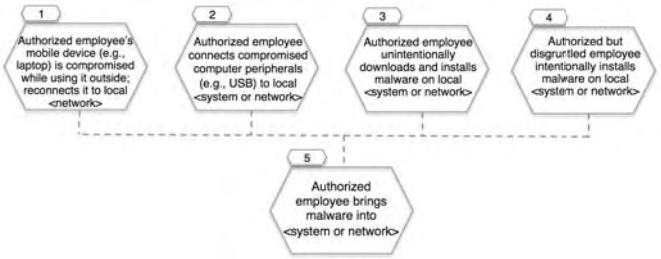
공격자는 통신을 필요로 하는 두 노드 간의 무선 통신 채널에서 메시지가 전달되지 못하도록 한다; 이는 본질적으로 통신 속도를 저하시킴으로써 통신이 중지되는 것과 동일한 효과를 보이는 것과 같다. 기본적으로 인터넷 상에서 데이터가 전달되는 것은 유선으로 연결된다. 두 개의 노드 x 와 y 가 무선으로 연결된다는 것은, 일반적으로, 스마트 그리드를 위한 에너지 관련 장비와 무선 공유기 사이의 통신을 의미한다. 이러한 환경에서, "송신자"와 "수신자"라는 용어는 데이터를 주고 받는 노드의 역할을 지칭하는 의미로만 해석된다. 그림 3 은 (B) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 3) (B) 위협에 대한 공격 트리 다이어그램.

Authorized Employee Brings Malware into <system or network>.

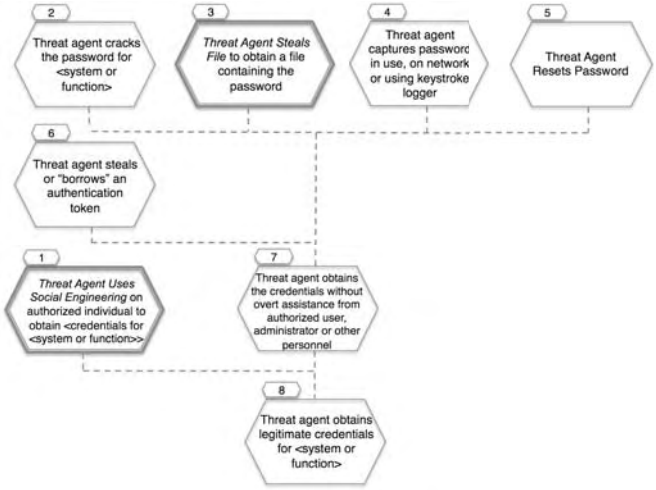
공식적으로 권한이 부여된 직원이 회사의 IT 인프라를 사용하며, 이로 인해 (의도적이든, 비의도적이든) 외부의 악성코드가 스마트 그리드 관련 네트워크/시스템에 침투할 수 있게 된다. 기본적으로 이러한 IT 인프라 또는 내부 네트워크는 방화벽이나 포트/IP 주소 제한과 같이 수단으로 보호되고 있는게 일반적인 설정이다. 그렇지만, 내부 네트워크에 연결된 하나의 기기가 악성코드에 감염된다면, 이는 또다른 내부 시스템을 감염시킬 수 있다. 감염된 기기는 일반적으로 외부에 있는 공격자가 원격으로 조정할 수 있는 상황이 된다. 그림 4 는 (C) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 4) (C) 위협에 대한 공격 트리 다이어그램.

Threat Agent Obtains Credentials for <system or function>.

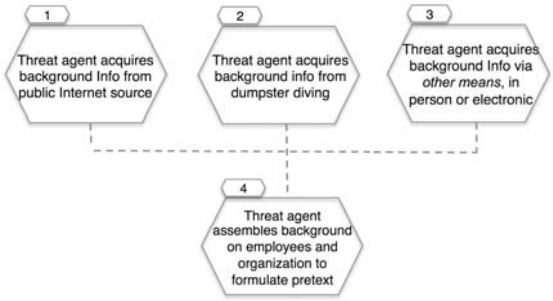
공격자는 시스템에 접근할 수 있는 공식적인 권한이나 특정 기능을 수행하기 위한 권한을 제공하는 자격 증명을 여러 가지 방법으로 얻을 수 있다. 이러한 기능은 공격자들이 찾고, 훔치거나, 추측하거나, 변경하는 것이 포함된다. 공격자는 이러한 방법을 수행하기 위해 사회 공학 기술을 사용할 수 있다. 자격 증명에 사용되는 각 기술 및 구현은 일부 방법에 내성이 강하고 다른 방법에 취약할 수 있다. 자격 증명의 예로는 정적 데이터 (암호) 또는 실제 개체 (예를 들어, 토큰이라고 하는 키 카드)들이며, 이것들은 현재 일반적인 인증 방식 중 하나로 널리 이용되고 있다. PIN 이 있는 토큰과 같은 2 단계 인증이 사용되는 경우 공격자는 자격 증명의 모든 "요소"을 얻기 위해 더 많은 단계를 수행해야 한다. 그림 5 는 (D) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 5) (D) 위협에 대한 공격 트리 다이어그램.

Threat Agent Uses Social Engineering to <desired outcome>.

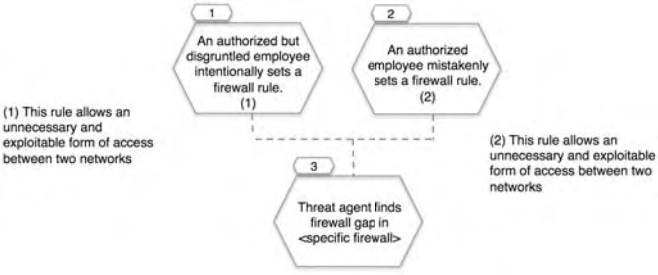
공격자는 임의의 내부 구성원을 설득하여 공범자로 만들기 위해 사회 공학 기법을 사용할 수 있다. 공범자로 하여금 공격자에게 이익이 되는 결과를 가져 올 수 있는 행동을 하도록 한다. 일반적인 행동의 예로는 특정 정보를 공개하거나, 정보를 수집하거나, 공범자가 속한 IT 인프라에 해를 끼치는 소프트웨어를 설치하고 실행하는 것이다. 그림 6 은 (E) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 6) (E) 위협에 대한 공격 트리 다이어그램.

Threat Agent Exploits Firewall Gap in <specific firewall>.

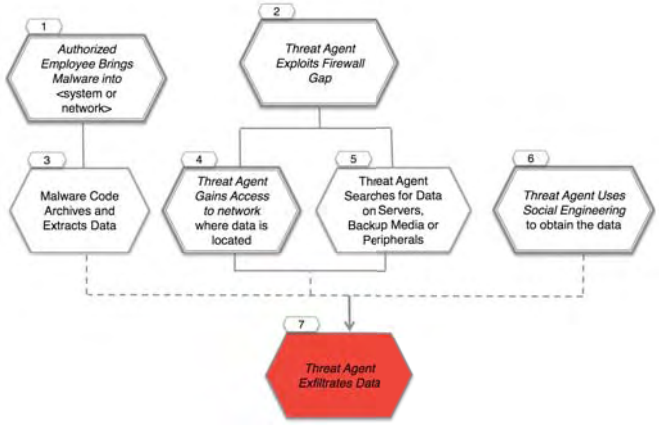
공식적으로 권한이 부여된 직원이 (실수로 또는 의도적으로) 방화벽 규칙을 설정함으로써, 외부에 있는 공격자가 내부 네트워크에 접근할 수 있는 불필요하고 악용 가능한 형태의 액세스를 허용할 수 있다. 그림 7 은 (F) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 7) (F) 위협에 대한 공격 트리 다이어그램.

Threat Agent Exfiltrates <data>

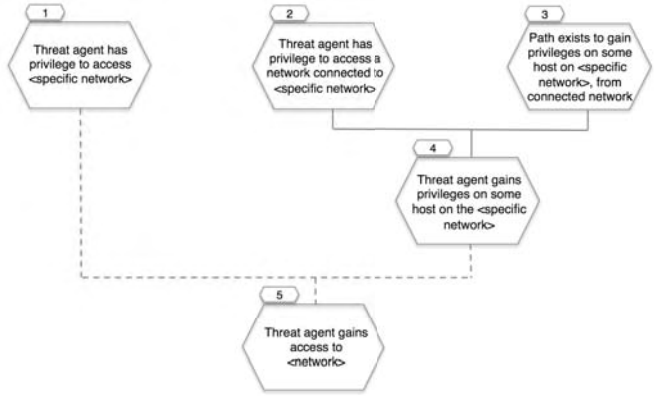
공격자는 직접 또는 간접적인 방법을 사용하여 내부 파일 또는 데이터의 복사본을 획득하여 외부로 유출시킬 수 있다. 방법의 예로는, 파일을 저장하고 있는 시스템으로의 직접 침입, 백업 미디어에서 데이터 찾기, 프린터와 같은 주변 장치 스캔 및 소셜 사용 등 피해자가 데이터를 제공하도록 영향을 줄 수 있는 사회 공학적 방법 등을 포함한다. 그림 8 은 (G) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 8) (G) 위협에 대한 공격 트리 다이어그램.

Threat Agent Gains Access to <network>

공격자는 내부 네트워크 내에서 트래픽을 전송하고 상주하는 호스트 시스템과 통신을 시도 할 수 있다. 이러한 위협에 대한 가장 강력한 예방은 스마트 그리드 네트워크를 일반 데이터 네트워크와 완전히 분리하는 것이다. 차선책은 강력한 최소 권한 법칙을 적용하는 것이다. 그림 9 는 (H) 위협에 대한 공격 트리 다이어그램을 나타낸다.



(그림 9) (H) 위협에 대한 공격 트리 다이어그램.

4. 결론

현대 사회의 대표적인 자원 기간망인 전력망을 현대화하는 스마트 그리드는 사소한 사이버 보안 실패만으로도 우리 사회 전체에 영향을 줄 수 있으며, 이로 인해 사이버 보안 기술에 많은 관심이 가지고 있다. 본 논문에서는 다양한 스마트 그리드 세부 도메인에서 공통적으로 발생할 수 있는 보안 위협 상황을 도출하고, 이러한 상황이 발생될 수 있는 공격 트리를 도식화 한다. 도출된 8 개의 공격 트리는 스마트 그리 분야에서 사이버 보안 기술 적용을 위한 근본적인 접근 방식에 대한 방향 설정을 위해 활용될 수 있을 것으로 기대한다. 보안 위협 상황을 예방하기 위한 전략과 실현 기술에 대한 실험은 좋은 미래 연구 방향의 하나가 될 것이다.

Acknowledgement

본 연구는 2016 년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (20162010103900) 교신저자는 이은규.

참고문헌

[1] V. Pillitteri and T. Brewer, Guidelines for Smart Grid Cybersecurity, National Institute of Standards and Technology Interagency Report (NISTIR 7628) Revision 1, Sep. 2014.

[2] Framework and Roadmap for Smart Grid Interoperability Standards, R3.0, NIST Special Publication 1108r3, Sep. 2014.

[3] U.S. Department of Defense, "Defense Acquisition Guidebook", Section 8.5.3.3.

[4] Electric Sector Failure Scenarios and Impact Analyses - National Electric Sector Cybersecurity Organization Resource (NESCOR), Dec. 2015. See http://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf

[5] A. Lee, et al., NESCOR Attack Tree, Dec. 2015. See http://smartgrid.epri.com/doc/NESCOR%20Attack%20Trees%2012-11-15.pdf

[6] C. Ten, C. Liu, M. Govindarasu, Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees, IEEE Power Engineering Society General Meeting, June 2007.