결함-공격 트리 기반 안전성 및 보안 분석 기법 비교*

조은호º, 신용준, 지은경, 배두환
한국과학기술원
{ehcho, yjshin, ekjee, bae}@se.kaist.ac.kr

Comparative Analysis of fault-attack tree based safety and security assessment approaches

Eunho Cho, Yong-Jun Shin, Eun-Kyoung Jee, Doo-Hwan Bae
School of Computing, Korea Advanced Institute of Science and Technology(KAIST)

요 약

시스템의 안전성과 보안은 시스템이 결함이나 의도하지 않은 행동을 나타내지 않도록 막는 두 축이다. 다양한 시스템이 인터넷과 연결되면서, 안전성과 보안이 동시에 요구되고 있다. 안전성과 보안은 상호보완작용 관계에 있기 때문에, 시스템의 안전성과 보안 분석을 하나로 통합하여 효율성을 높이는 시도가 전개되고 있다. 안전성 분석 기법의 하나인 결합 트리와 보안 분석 기법의 하나인 공격 트리를 통합하여, 결함-공격 트리 형태의 기법을 제안하고, 시스템을 분석하는 연구가 그중 하나이다. 결함-공격 트리 기반 분석은 정량적, 정성적 분석이 모두 가능하고, 시스템을 직관적으로 이해하고 분석하기 쉽다는 장점이 있으나, 일치된 표기 방식이나 기법이 정립되어 있지 않은 상황이다. 본 연구에서는 결함-공격 트리를 제안하거나 활용한 연구를 비교·분석함으로써, 결함-공격 트리 기반 분석 기법의 현황과 발전 방향을 제시한다.

1. 서론

시스템 내부 요소의 오작동을 결함, 악의적인 목적을 가지고 시스템 내•외부에서 오작동을 유도하는 것을 공격이라고 할 때, 시스템 내부의 의도하지 않은 결함을 방지하는 수준을 의미하는 안전성과 시스템 내•외부의 공격을 방어하는 수준을 의미하는 보안은 시스템이 결함이나 의도하지 않은 행동이 일어나지 않도록 막는 두 축이다. 국제자동제어협회(International Society of Automation, ISA)는 안전성과 보안의 표준으로 각각 ISA84(IEC 61511)과 ISA99(IEC 62443)를 제시하여, 시스템의 안전성과 보안을 관리하고 있다[1].

사회 기반시설부터 일상생활에서 자주 쓰이는 물품까지 다양한 시스템이 인터넷과 연결되면서, 안전성과 보안이 동시에 요구되는 시스템이 늘어나고 있고, 이러한 시스템들에서 안전성과 보안은 상호보완적인 관계에 있어[4], 안전성에 위협이 발생하면 보안에도 함께 위협이 발생할 수 있고, 보안에 위협이 발생하면 안전성에도 함께 위협이 발생할 수 있다. 이에 따라, 안전성과 보안 취약점 분석의 과정에서 서로를 고려할 필요성이 대두되었고, 과정과 결과를 하나로 통합하여 효율성을 높이려는 연구들이 진행되고 있다[1-3, 5].

안전성 분석 기법 중 많이 쓰이는 결함 트리(Fault Tree)의 장점과 보안 취약점 분석에서 많이 쓰이는 공격 트리(Attack Tree)의 장점을 통합하여 결함-공격 트리(Fault-Attack Tree)를 구축하고 이를 기반으로 분석하는 연구가 그중 하나이다. 결함-공격 트리 기반 분석은 트리를 통해 정량적 분석과 정성적 분석이 모두 가능하고, 직관적으로 이해하기 쉽다는 장점이 있다.

하지만, 아직 결함-공격 트리에 대한 통일된 표기법이 없는 등 기법이 안정화되지 못한 상황이다. 본 논문에서는 결함-공격 트리 기법 관련 연구를 분석하고, 발전 방향을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 결함-공격 트리 관련 연구를 소개한다. 3장에서는 결함-공격 트리 관련 연구를 비교 분석하고, 관련 이슈들을 도출한다. 4장에서 결론 및 향후 발전 방향을 제시한다.

2. 결함-공격 트리 관련 연구

2.1 사이버물리시스템(CPS)의 안전성과 보안 표준 통합 구축

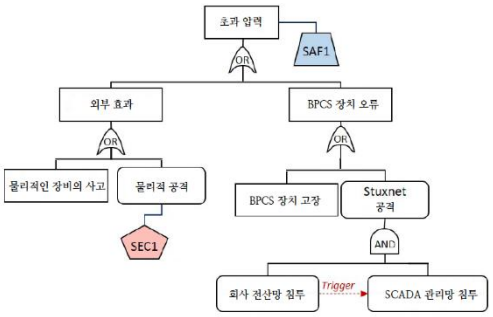

그림 1. FACT 그래프 예시

Sabaliauskaite 외[1]의 연구에서는 ISA84와 ISA99로 대표되는 안전성과 보안의 두 표준을 통합하여 구축하고자 하였다. 두 표준에서 설명하는 안전성과 보안 취약점 분석 및 방비의 과정을 하나로 통합하고, 그 과정에서 사용되는 결함 트리나 공격 트리와 같은 기법의 결과물을 하나로 통합하여 FACT(Failure, Attack, CounTermeasure) 그래프를 만들어 분석과 방비에 활용하였다. 그림 1은 Sabaliauskaite 외[1]의 연구에 제시된 예시의 일부로, 송수관의 초과 압력 상황에 대한 FACT 그래프를 나타낸 것이다. FACT 그래프는 결함 트리를 기반으로 하여, 공격 트리의 목표에 해당하는 결함에 결합하고, 그래프에 표현된 결함이나 공격을 방어할 수 있는 대비책(Countermeasure)을 나타내는 순서로 만들어진다. 그래프를 만드는데 필요한 결함

* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업(2016-0-00018)과 국제협력 R&D 프로젝트 CybWin(Project Number: 287808)의 연구결과로 수행되었음

트리나 공격 트리는 단순한 AND, OR 게이트와 Fault, Attack 노드만 사용되며, 부분적으로 공격의 순서를 나타낼 때, Trigger 게이트를 사용한다. Sabaliauskaite 외[1]의 연구는 표준의 통합에 초점을 맞추었으며, 그래프에 대한 분석 기법은 제시되지 않았다

2.2 결함 트리 기반 사이버 공격의 표현 및 통합

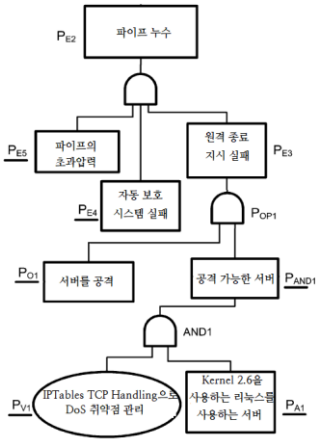

그림 2. 확장 결함 트리 예시

Forvino 외[2]의 연구에서는 결함 트리와 공격 트리를 정형적으로 자세히 정의하고, 결함 트리에, 공격 트리를 결합한 확장된 결함 트리(Extended Fault Tree, EFT)를 제시하고, EFT 에 대한 정량적 분석 방법을 제시하였다. 그림 2 는 Forvino 외[2]의 연구에 제시된 예시의 일부로, 파이프 누수 상황에 대한 EFT 를 나타낸다. 결함 트리를 기반으로 하고, 공격 트리를 목표로 하는 특정 결함에 결합한다는 점에서 EFT 는 Sabaliauskaite 외[1]의 연구와 유사하나, 결합하는 방법을 보다 정형적이고 구체적으로 기술하고 있다. 먼저, 같은 결함을 목표로 가지는 다수의 공격 트리를 OR 게이트를 통해 하나로 통합한다. 통합된 공격 트리는 추가적인 OR 게이트를 통해 목표로 하는 결함에 연결되어 있던 기존 부분 트리와 결합하여 EFT 를 구성하게 된다. EFT 를 구성하는 게이트의 종류는 기본적인 결함 트리와 같으나, 구성하는 공격 트리의 노드가 Vulnerability, Assertion, Operation 등으로 다양하다는 차이가 있고, 시간 개념이 포함되지 않은 정적 트리만을 대상으로 한다. EFT 기법에서는 각 노드에 확률을 정의하고, 그 확률에 기반하여 정량적 분석을 수행한다. OR, AND 게이트 관련 확률 계산은 일반적인 방법을 따른다.

2.3 공격-결함 트리를 이용한 안전성 및 보안 정량 분석

Kumar 외[3]의 연구는 동적 결함 트리에 공격 트리를 결합한 형태인 결함-공격 트리를 제안한다. 해당 결함-공격 트리를 확률적 타임드 오토마타(Stochastic Timed Automata, STA)형태로 변환한 후, UPPAAL 을 통해 정량적 분석을 수행하였다. 동적 결함 트리와 공격 트리를 통합하는 상세 절차는 제시되어 있지 않다. 그림 3 은 Kumar 외[3]의 연구에 제시된 예시의 일부로, 송유관의 고장으로 인한 오염에 대한 공격-결함 트리 일부를 나타낸 것이다. 동적 결함 트리의 게이트인 PAND, FDEP, SPARE 를 비롯하여 Sabaliauskaite 외[1] 연구에서의 Trigger 와 같은 역할을 하는 SAND, 결함 트리의 확장된 게이트인 VOT(*k*)/*n* 도 포함하는 폭넓은 표현력을 가지고 있다. 노드 역시 결함을 시간에 따른 지수 함수의 확률로 일으키는 Basic

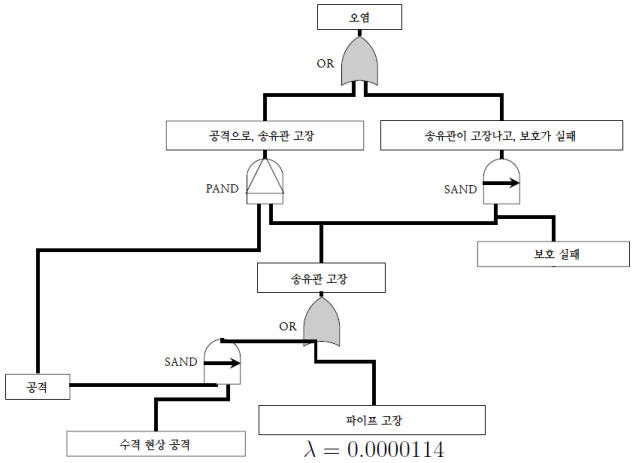

그림 3. 공격-결함 트리 예시

Component Failure(BCF)와 숫자 값의 확률로 일어나는 Instant Failure(IF)로 구분하고 있다. Kumar 외[3]의 연구에서는 결함-공격 트리의 노드와 게이트를 각각의 STA 로 나타내고, 각각의 STA 를 통합한 오토마타를 만들어, UPPAAL 을 통해 분석한다. 특정 시간에서의 결함 발생 확률, 결함까지의 평균 시간 등을 정량으로 분석하였다.

3. 결함-공격 트리 관련 연구 분석

3.1 절에서 결함-공격 트리 관련 연구를 비교하고, 이를 바탕으로 이슈들을 3.2 절에서 분석한다.

3.1 결함-공격 트리 관련 연구 비교

표 1. 결함-공격 트리 기법 비교 분석

평가 기준 / 관련 연구	Sabaliauskaite 외[1](A)	Forvino 외[2](B)	Kumar 외[3](C)
통합 방식	결함 트리 + 공격 트리 + 대비책	결함 트리 + 다수의 공격 트리	다루고 있지 않음
정적/동적	부분 동적	정적	동적
포함하는 노드의 종류	Event, Attack	Event, Vulnerability, Assertion, Operation	BCF, IF, Attack
포함하는 게이트의 종류	AND, OR, Transfer, Trigger	AND, OR	AND, OR, VOT(k)/n, PAND, FDEP, SPARE, SAND
대비책	트리에 포함	포함하지 않음	포함하지 않음
정량적 분석 지원	지원하지 않음	숫자 값 확률 기반	시간에 따른 지수함수 확률 기반
자동화 도구 지원	지원되지 않음	지원되지 않음	지원되지 않음

2 장에서 소개된 3 가지 관련 연구를 평가 기준에 따라 비교 분석한 결과를 표 1 에 정리하였다. Sabaliauskaite 외[1]의 연구와 Forvino 외[2]의 연구는 트리의 통합 방식과 알고리즘에 관하여 다루었으며, 모두 결함 트리를 기반으로 공격 트리를 특정

결함에 결합하는 방식으로 통합한다. Forvino 외[2]의 연구에서는 공격 트리를 해당하는 결함에 통합하며, Sabaliauskaite 외[1]의 연구는 구체적으로 OR 게이트를 통해 공격 트리를 결함 트리에 결합하는 방법을 제안하였다.

Forvino 외[2]의 연구 결과로 통합된 트리는 정적 트리였으나, Sabaliauskaite 외[1]의 연구에서는 Trigger 라는 형태를 통해 부분적으로 순서와 시간 개념을 Tree 에 포함했으며, Kumar 외[3]의 연구는 동적 결함 트리를 기반으로 하여 동적 트리를 기반으로 분석하였다. 각 연구에서 표현하는 노드와 게이트의 종류도 다양하였다. 표기된 결함이나 공격에 대한 대비책이 표기된 것은 Sabaliauskaite 외[1]의 연구가 유일했다. 다른 두 연구에서는 정량적 분석을 목표로 하여 대비책에 관한 언급은 없이 숫자 값의 확률을 기반한 계산과 시간에 따른 지수함수의 확률을 기반한 계산을 통한 정량 분석 방식을 제안하였다.

소개된 결함-공격 트리 기반 기법 모두 직관적으로 시스템의 안전성과 관련된 요소들을 보여주는 결함 트리의 장점과 해당 요소에 해당하는 공격을 보여주어 방어하기 용이하도록 하는 공격 트리의 장점을 포함한다는 장점이 있다.

3.2 결함-공격 트리 관련 이슈

3.2.1 일관되지 않은 표기 방식

결함-공격 트리 기반 분석 관련 연구들 모두 각각의 표기법에 기반한 결함 트리, 공격 트리에 따라 표기법이 다르고, 표현할 수 있는 범위가 다르다. 표현 가능한 노드와 게이트의 종류가 많을수록 표현력이 향상되고, 복잡한 시스템을 더 구체적으로 표현할 수 있다는 장점이 있다. 하지만, 결함 트리의 장점인 직관적으로 이해하기 쉽다는 장점이 약화하게 되며, 정성적, 정량적 분석이 더 복잡해진다는 단점이 있다. 노드와 게이트의 종류가 적은 경우, 반대로 표현력이 작아지지만, 정성적, 정량적 분석이 더 쉽고 빠르게 진행된다는 장점이 있다. 다양한 표기 방식을 상황에 맞게 사용하기 위해서, 표기법을 필수적인 요소와 부가적인 요소로 구분하여 체계적으로 분류하고 활용하는 가이드라인의 정립이 필요하다.

3.2.2 정량적 분석 기법 미비

3.1 절에서 비교한 연구들에서 제시된 결함-공격 트리 대상 정량적 분석 기법은 기존 결함 트리의 정량적 분석 기법을 사용하는 것이다. 하지만, 공격 트리의 분석 기법과 결함 트리의 분석 기법이 다르게 발전되어 왔으며, 그 대상과 방식에 차이가 있어, 결함-공격 트리에 결함 트리의 분석 기법을 그대로 적용하는 것이 적절하지 않을 수 있다. 결함-공격 트리 기반 정량적 분석 기법을 개발하고, 이를 실제 사례 등을 통하여 검증할 필요가 있다.

3.2.3 관련 도구의 부재

결함-공격 트리 기반 기법이 산업 현장에서 효과적으로 활용되기 위해서는 자동화 도구의 지원이 중요하다. 그러나, 결함-공격 트리 작성이나 분석 기법을 제안한 연구 어디에서도 자동화 도구 지원 여부를 찾을 수 없었다. 현재, 결함 트리와 공격 트리에 대해서는 다양한 도구가 개발되어 있어, 실제 산업 현장에서 사용하기에 문제가 없지만, 결함-공격 트리의 작성이나 분석을 지원하는 도구는 미비한 상황이다.

Fault Tree+[6]와 같은 상업용 도구는 결함 트리의 확장 형태로 부분적으로 표현할 수 있지만, 오픈소스 도구만을 사용할 경우, 표현이 어렵다. 결함-공격 트리를 지원하는 도구는 정량적 분석은 물론, 기존 결함 트리에서 사용되는 최소 절단 집합(Minimal Cut Set)과 같은 정성적인 분석도 지원하여 실제 산업 현장의 요구를 충족할 필요가 있다.

결함-공격 트리라는 개념이 비교적 최근에 등장하였기 때문에, 결함-공격 트리를 설계하는 방식이나, 안전성, 보안 절차 중 어느 단계에서 설계할지와 관련된 체계가 아직 마련되어 있지 않은 상황이다. 실제 산업 현장에서 결함 트리와 공격 트리가 익숙하다는 점과 안전성 및 신뢰성 전문가, 보안 전문가가 분리되어 있음을 고려하여, 결함-공격 트리는 이미 작성되어 있는 결함 트리와 공격 트리를 기반으로 통합하는 것이 효율적이라 할 수 있다. 이러한 통합을 돕기 위하여, 결함 트리, 공격 트리가 특정 조건을 만족하였을 때, 자동으로 통합하는 기술 개발을 고려할 수 있다.

4. 결론

본 논문에서는 결함-공격 트리를 기반으로 하여 시스템의 안전성과 보안을 통합적으로 분석하는 기법을 비교 분석하고, 실제로 결함-공격 트리를 산업에서 활용하고자 할 때에 발생할 수 있는 이슈들을 도출하였다. 현재까지의 결함-공격 트리는 안전성과 보안을 분석하는 결함 트리와 공격 트리의 장점을 모두 포함하는 기법으로 발전되어 왔다. 하지만, 개념의 제시가 오래되지 않아, 표기 방식이 일관되지 않고, 정량적 분석 기법이 체계화 되지 않았으며, 자동화 도구 지원이 미비하다.

본 논문에서 보인 비교 분석에 기반하여 향후 연구에서는 결함 트리와 공격 트리를 결함-공격 트리로 체계적으로 통합하는 방법을 제안하고, 정량, 정성적 분석을 지원하는 오픈소스 자동화 도구를 개발하고자 한다.

참고 문헌

[1] Sabaliauskaite, Giedre, and Aditya P. Mathur. "Aligning cyber-physical system safety and security." *Complex Systems Design & Management Asia*. Springer, Cham, 2015. 41-53.

[2] Fovino, Igor Nai, Marcelo Masera, and Alessio De Cian. "Integrating cyber attacks within fault trees." *Reliability Engineering & System Safety* 94.9 (2009): 1394-1402.

[3] Kumar, Rajesh, and Mariëlle Stoelinga. "Quantitative security and safety analysis with attack-fault trees." *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, 2017.

[4] Dariz, Luca, et al. "Trade-off analysis of safety and security in CAN bus communication." *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. IEEE, 2017.

[5] Piètre-Cambacédès, Ludovic, and Marc Bouissou. "Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes)." *2010 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2010.

[6] "FaultTree+." Isograph, www.isograph.com/software/reliability-workbench/fault-tree-analysis-software/.