



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월16일
(11) 등록번호 10-2444922
(24) 등록일자 2022년09월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) G06F 21/57 (2013.01)
G06N 5/04 (2006.01)
(52) CPC특허분류
H04L 63/302 (2013.01)
G06F 21/57 (2013.01)
(21) 출원번호 10-2021-0056590
(22) 출원일자 2021년04월30일
심사청구일자 2021년04월30일
(56) 선행기술조사문헌
KR1020140083336 A*
US20150222666 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
최준호
광주광역시 서구 염화로57번길 16, 101동 1205호
(화정동, 중흥아파트)
김형주
광주광역시 동구 중앙로160번길 16-33(호남동)
(74) 대리인
특허법인 남앤남

전체 청구항 수 : 총 7 항

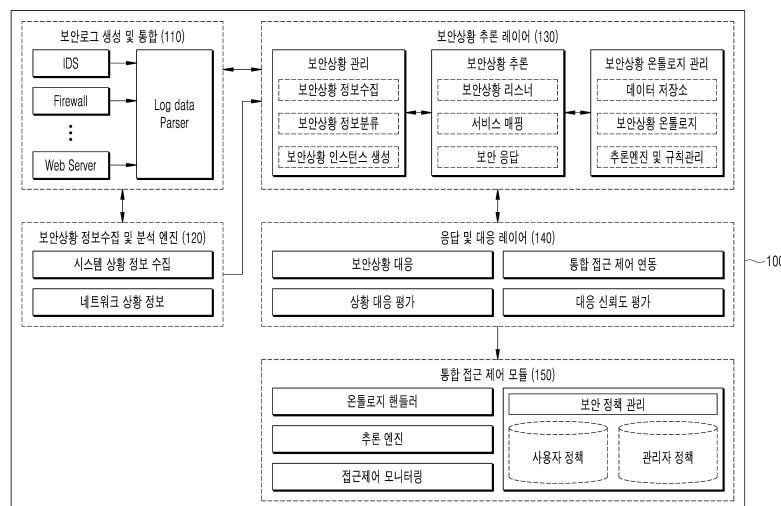
심사관 : 홍기완

(54) 발명의 명칭 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치

(57) 요약

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치가 개시된다. 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치는 전력 시스템 내 다수의 보안 시스템의 로그 데이터를 설정된 분석 가능한 형태로 변환하고, 변환된 로그 데이터에서 불필요한 데이터를 삭제하고, 설정된 조건을 만족하는 유용한 데이터를 추출하는 보안 로그 생성 및 통합 모듈과, 전력시스템의 네트워크 및 전력시스템이 정상 작동 상태에서 실행 중인지를 결정하는 보안상황 정보수집 및 분석 엔진 모듈과, 온톨로지 추론기술을 적용하여 전력시스템의 보안상황 정보를 수집하고, 분석하여 전력시스템의 보안상황 인식서비스를 제공하는 보안상황 추론 레이어 모듈을 포함할 수 있다.

대표도



(52) CPC특허분류

G06N 5/04 (2013.01)

H04L 63/10 (2013.01)

H04L 63/1408 (2013.01)

명세서

청구범위

청구항 1

다수의 보안 시스템에 의해 보호되는 전력 시스템을 제어하는 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치로서,

상기 전력 시스템 내 다수의 보안 시스템의 로그 데이터를 수집하여 설정된 분석 가능한 형태로 변환하고, 상기 분석 가능한 형태의 로그 데이터로부터 미리 설정된 조건을 만족하는 보안 데이터를 추출하는 보안 로그 생성 및 통합 모듈;

추출된 상기 보안 데이터에 기초하여 상기 전력 시스템의 네트워크 및 상기 전력 시스템이 정상 작동 상태에서 실행 중인지 보안위협 상태에서 실행 중인지를 결정하는 보안상황 정보수집 및 분석 엔진 모듈; 및

상기 전력 시스템의 네트워크 및 상기 전력 시스템이 보안위협 상태에서 실행 중인 것으로 결정된 경우, 온톨로지 추론기술을 적용하여 상기 전력 시스템의 보안상황 정보를 수집하고, 분석하여 상기 전력시스템의 보안상황 인식서비스를 제공하는 보안상황 추론 레이어 모듈을 포함하고,

상기 온톨로지 추론기술은 상기 전력 시스템 내 보안 시스템으로부터의 상기 보안 데이터에 대한 로그 구조 분석을 포함하되,

보안 로그 생성 및 통합 모듈은,

상기 전력 시스템에서 발생하는 보안 사건을 표현하는 방법 또는 상기 전력 시스템의 네트워크 트래픽을 분석하여 감지된 이벤트를 나타내는 메시지 교환을 위해, IDMEF(침입 탐지 메시지 교환 형식) 포맷을 신뢰도 섹션을 포함하도록 확장하되,

상기 신뢰도 섹션은,

보안상황 경보를 발생시킨 보안 시스템에 대한 신뢰도 및 상기 신뢰도를 계산하는데 사용되는 알고리즘에 대한 정보를 포함하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 신뢰도 섹션은 상기 전력 시스템에 보안 공격이 진행 중인 확률을 나타내는 공격확률 및 상기 보안상황 경보에 대한 신뢰 점수, 상기 신뢰 점수를 계산하는 노드에 대한 정보를 더 포함하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

청구항 4

제3항에 있어서,

상기 보안 상황정보는 네트워크 보안 상황정보 및 시스템 보안 상황정보를 포함하고,

상기 네트워크 보안 상황정보는,

상기 전력 시스템 내 서버 네트워크의 트래픽에 대한 스냅샷, 현재 시간, 날짜, 프로토콜 유형, IP 주소, 포트, IP 대상 주소, 대상 포트, 트래픽 매개 변수, 수신 및 전송된 바이트 중 적어도 하나를 포함하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

청구항 5

제3항에 있어서,

상기 보안상황 추론 레이어 모듈은,

상기 전력시스템 내 각종 보안 시스템의 로그 구조 분석을 통하여 상기 보안상황 정보를 획득한 후, 상기 보안 상황 정보에 상기 온톨로지의 규칙기반 추론 엔진에 의한 추론을 적용하여, 상기 전력시스템의 보안상황 인식서 비스를 제공하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

청구항 6

제1항에 있어서,

상기 보안상황 추론 레이어 모듈은,

설정된 보안상황 분석 엔진을 이용하여, 공격 상태를 감지하기 위해 공격 전후의 보안상황 정보를 기반으로 공격단계, 침투단계 및 수집단계 중 어느 하나의 단계인지를 추론하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

청구항 7

제1항에 있어서,

상기 전력시스템의 보안상황 인식 서비스에서 공격 대응 방안을 추론하고, 상기 추론의 결과에 대한 피드백을 생성하고 보안 공격에 대한 경고를 발생시킨 보안 시스템의 신뢰도를 평가하는 응답 및 대응 레이어 모듈을 더 포함하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

청구항 8

제1항에 있어서,

상기 보안 데이터에 기초한 사용자 인증, 상기 전력 시스템으로의 접근제어 및 상기 보안상황 정보 중 적어도 하나를 관리하는 지능형 통합 접근제어 모듈을 더 포함하는,

스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치.

발명의 설명

기술 분야

- [0001] 본 발명은 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 기술에 관한 것이다.
- [0002] 본 발명은 하기와 같은 연구과제의 지원을 받아 수행된 연구 결과이다.
- [0003] [과제고유번호]R18XA06-12(한국전력공사 과제번호)
- [0004] [과제번호]2020-0651(조선대학교 산학협력단 과제번호)
- [0005] [연구관리전문기관]한국전력공사
- [0006] [연구사업명]한국전력공사 사외공모 기초연구
- [0007] [연구과제명]스마트그리드 환경에서 온톨로지 기반 전력시스템 보안 상황인식을 이용한 지능형 통합 접근제어 시스템 개발
- [0008] [주관기관]조선대학교 산학협력단
- [0009] [연구기간]2018-05-01~2021-04-30(총 36 개월)

배경 기술

- [0010] 스마트그리드(Smart Grid)란 기존의 전력망에 ICT 기술이 결합한 지능형 전력기술로, 공급자와 소비자가 양방향으로 실시간 에너지 사용정보를 교환함으로써 에너지효율을 최적화시켜 주는 차세대 전력 인프라기술임. 스마트그리드는 재생에너지 보급을 위한 인프라를 구축함으로써 산업 전반에 걸쳐 큰 파급효과를 가져올 수 있는 신성장동력을 제공하고 있다.
- [0011] 스마트그리드에는 AMI(Advanced Metering Infrastructure), IoT 기술, 스마트 미터 기술, HAN(Home Network Area), 클라우드 컴퓨팅 등의 다양한 최신 ICT 기술이 접목되고 있지만, 다양한 사이버 공격에 노출될 것으로 전망되고 있고, 공격이 전력시스템에 가해지면 기존 정보통신 분야의 피해 규모보다 방대한 국가적인 피해를 유발할 가능성이 있다.
- [0012] 스마트그리드에서 개인정보 유출, 정전사태 등 공격의 종류가 다양해지고, 공격의 수준이 높아지고 있다. 전력공급의 중추인 스마트그리드 환경에서의 사이버 공격은 국가 전력 마비와 같은 심각한 피해를 주게 된다. 스마트그리드를 대상으로 하는 공격 방법이 다양해지고, 지능화되는 추세로 이에 대한 대응책으로 통합적이고, 지능적인 보안기술이 필요하다.
- [0013] 전력시스템에서의 기존 보안 침해사고 탐지 및 대응 기술은 일반적으로 패턴 기반과 행위 기반 등의 통계적인 방법이 주로 사용되었는데, 이는 갈수록 지능화, 다형성 성격을 갖는 보안 침해 공격에 대한 근본적인 해결책이 될 수 없다. 기존 패턴 기반의 침입 탐지 방법은 새로운 침입이나 전력시스템의 대용량 보안 로그 데이터를 생성하는 상황에서는 탐지율이 현격히 떨어지는 단점이 있다.
- [0014] 대규모 전력시스템 내 시스템 간의 관계와 보안상황, 시스템 보안, 접근제어 정책 등의 온톨로지를 구축한 후, 추론규칙을 정의하여 전력시스템 내 보안 사고가 발생하였을 때, 정확한 판단과 신속한 처리를 수행할 수 있는 지능형 보안 체계가 필요하다.

발명의 내용

해결하려는 과제

- [0015] 본 발명의 일실시예는, 전력시스템에서 발생하는 다양한 보안 침해사고에 대한 명확한 판단과 신속한 대응을 위해 보안상황 온톨로지를 설계하고, 이를 기반으로 추론규칙과 제약 조건을 정의한 후, 이를 전력시스템에 실제 적용할 수 있는 방법을 제공하는 것을 목적으로 한다.
- [0016] 본 발명의 일실시예는, 스마트그리드 환경의 전력시스템에 도입함으로써 각 전력서비스에 제한적으로 구현되고 있는 현재의 취약한 보안에 대해 안전하고 신뢰성 있는 전력서비스 생태계를 구축하는 데 활용이 가능한 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 기술을 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0017] 본 발명의 일실시예는 전력 시스템 내 다수의 보안 시스템의 로그 데이터를 설정된 분석 가능한 형태로 변환하고, 변환된 로그 데이터에서 불필요한 데이터를 삭제하고, 설정된 조건을 만족하는 유용한 데이터를 추출하는 보안 로그 생성 및 통합 모듈과, 전력시스템의 네트워크 및 전력시스템이 정상 작동 상태에서 실행 중인지를 결정하는 보안상황 정보수집 및 분석 엔진 모듈과, 온톨로지 추론기술을 적용하여 전력시스템의 보안상황 정보를 수집하고, 분석하여 전력시스템의 보안상황 인식서비스를 제공하는 보안상황 추론 레이어 모듈을 포함하는, 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치일 수 있다.
- [0019] 전술한 것 외의 다른 측면, 특징, 이점이 이하의 도면, 특허청구범위 및 발명의 상세한 설명으로부터 명확해질 것이다.

발명의 효과

- [0020] 본 발명의 실시예들에 의하면, 스마트그리드 환경의 전력시스템에 도입함으로써 각 전력서비스에 제한적으로 구현되고 있는 현재의 취약한 보안에 대해 안전하고 신뢰성 있는 전력서비스 생태계를 구축하는 데 활용이 가능하다.
- [0021] 본 발명의 실시예들에 의하면, 스마트그리드 환경에서 발생할 수 있는 보안 및 프라이버시 이슈를 체계적으로 정리하고, 보안 침해사고 대응 방법으로서 기존 보안 연구에서 단점으로 지적된 보안 침해사고의 지능적인 접근

제어를 통해 전력시스템의 보안 예방과 침입 방지 시스템에 적극적으로 활용할 수 있다.

[0022] 본 발명의 실시예들에 의하면, 스마트그리드 세계시장 규모가 점증적으로 확장될 것으로 전망됨에 따라, 전력시스템에 대한 지능형 보안 체계 구축 및 접근제어 방법을 활용하여 스마트그리드 보안 시장진출의 발판이 마련할 수 있다.

[0023] 본 발명의 실시예들에 의하면, 기존 패턴 기반 보안 대응 방법보다 향상된 결과를 제공할 수 있는, 보안상황 정보를 활용한 지능형 접근 제어기술을 스마트그리드 보안 관련 기업들이 구축하게 될 많은 스마트그리드 보안제품에 도입함에 따라, 개선된 보안 협업 환경과 규모 확장성에 크게 활용할 수 있다.

[0024] 또한, 본 발명의 실시예들에 의하면, 지능형 접근 제어기술을 각 공공기관, 기업 등의 보안 실무자의 침해사고 대응 업무에 효과적으로 활용할 수 있고, 내부 정보 유출 모니터링, 실시간 감사 모니터링 업무에도 크게 활용될 수 있으며, 보안상황 자동 분석에도 활용할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일실시예에 따른 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치의 구성 일례를 도시한 도면이다.

도 2는 경고 클래스의 일례를 도시한 도면이다.

도 3은 신뢰도 섹션의 일례를 도시한 도면이다.

도 4 및 도 5는 전력시스템 내 보안상황 정보를 기반으로 하는 온톨로지의 일례를 도시한 도면이다.

도 6은 침입 탐지 시스템 클래스의 데이터 속성(data properties)의 일례를 도시한 도면이다.

도 7은 보안상황 정보 온톨로지를 이용한 APT 공격단계 추론 규칙의 일례를 도시한 도면이다.

도 8은 보안상황 정보 온톨로지를 이용한 APT 침투단계 추론규칙의 일례를 도시한 도면이다.

도 9는 보안상황 정보 온톨로지를 이용한 수집단계 탐지를 위한 추론 규칙의 일례를 도시한 도면이다.

도 10은 지능형 접근제어 동작 시나리오의 일례를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 설명되는 실시 예를 참조하면 명확해질 것이다. 그러나 본 발명은 아래에서 제시되는 실시 예들로 한정되는 것이 아니라, 서로 다른 다양한 형태로 구현될 수 있고, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 아래에 제시되는 실시 예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0027] 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다. 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0028] 이하, 본 발명에 따른 실시 예들을 첨부된 도면을 참조하여 상세히 설명하기로 하며, 첨부 도면을 참조하여 설명함에 있어, 동일하거나 대응하는 구성 요소는 동일한 도면번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0030] 도 1은 본 발명의 일실시예에 따른 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치의 구성 일례를 도시한 도면이다.

[0031] 도 1을 참조하면, 본 발명의 일실시예에 따른 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치

(100)(이하, '지능형 접근제어 장치'로 칭함)는 다수의 보안 시스템에 의해 보호되는 전력 시스템을 제어하는 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치로서, 스마트그리드 환경 내에서 협업 가능한 프레임워크로 설계될 수 있다. 전력시스템의 관리자는 전력서비스 주체와 에이전트 사이에서 필요한 접근제어 정책 정보를 전달하는 역할을 하도록 설계될 수 있다.

[0032] 또한, 지능형 접근제어 장치(100)는 전력시스템이 요청하는 모든 접근에 대한 예외 상황(접근 거부, 오남용, 임계값 초과 등)에 대한 정보를 수집하여 보안 공격 패턴과 비교 분석 후 새로운 공격 패턴으로 판명되면, 해당 정보를 각 에이전트에게 통지하여 최적화된 지능형 접근제어 정책을 자동으로 생성할 수 있게 한다.

[0033] 지능형 접근제어 장치(100)는 전력시스템에 보안 침해 상황이 발생하면 에이전트에게 사고 발생 위치에 대한 정보를 공지하고, 정보를 갱신할 수 있다. 지능형 접근제어 장치(100)는 분석된 공격 패턴과 공격 의도를 판단하고, 전력시스템 내 접근제어 정책에 반영할 수 있다. 지능형 접근제어 장치(100)는 전력시스템의 보안상황을 모니터링하기 위해 마스터 서버에 배치되고, 호스트에서 주기적으로 작동하고, 시스템 성능을 저하시키지 않기 위해 일정한 시스템 자원효율을 유지할 수 있게 한다.

[0034] 지능형 접근제어 장치(100)는 보안상황 인식 서비스를 통해 보안 침해사고 징후 발생 시 보안 경고를 생성하고, 보안 침해 분석을 시행하기 위한 시스템으로 구현될 수 있다.

[0035] 이러한 지능형 접근제어 장치(100)는 보안 로그 생성 및 통합 모듈(110), 보안상황 정보수집 및 분석 엔진 모듈(120), 보안상황 추론 레이어 모듈(130), 응답 및 대응 레이어 모듈(140) 및 지능형 통합 접근제어 모듈(150)을 포함할 수 있다.

[0036] 보안 로그 생성 및 통합 모듈(110)은 전력 시스템 내 다수의 보안 시스템의 로그 데이터를 분석 가능한 형태로 변환하고, 분석 가능한 형태의 로그 데이터로부터 미리 설정된 조건을 만족하는 보안 데이터를 추출할 수 있다. 즉, 보안 로그 생성 및 통합 모듈(110)은 로그 데이터에서 불필요한 데이터를 삭제하고, 설정된 조건을 만족하는 유용한 데이터를 추출할 수 있다.

[0037] 보안 로그 생성 및 통합 모듈(110)은 다양한 형태로 구현될 수 있으나, 하기에서는 일 예를 설명한다.

[0038] 보안 로그 생성 및 통합 모듈(110)은 전력 시스템에서 발생하는 보안 사건을 표현하는 방법 또는 전력 시스템의 네트워크 트래픽을 분석하여 감지된 이벤트를 나타내는 메시지 교환을 위해 'RFC 4765'의 IDMEF(침입 탐지 메시지 교환 형식) 포맷을 신뢰도 섹션을 포함하도록 확장할 수 있다. IDMEF 데이터 모델은 이기종 보안 시스템의 탐지 메시지 교환 포맷으로 크게 두 종류의 메시지를 가질 수 있다. 해당 메시지는 도 2에 도시된 바와 같은, 네트워크 공격에 대한 탐지 정보를 포함하는 경고 클래스와 시스템의 동작상태 정보를 포함하는 동작상태 클래스로 나타낼 수도 있다.

[0039] 기존의 IDMEF 포맷은 시스템에서 보안상황이 발생했을 때, 보안상황 경보를 발생시킨 시스템에 대한 신뢰와 관련된 정보를 포함하지 않음에 따라, 본 발명에서의 IDMEF 포맷은 IDMEF 데이터 모델에 도 3에 도시된 바와 같은, 신뢰도 섹션을 확장하여 보안상황 경보를 발생시킨 보안 시스템에 대한 신뢰도(신뢰값, 신뢰 점수)를 포함할 수 있도록 정의될 수 있다. 즉, 신뢰도 섹션에 포함된 정보는 보안 시스템에 대한 신뢰도 및 신뢰도를 계산하는데 사용되는 알고리즘에 대한 정보 등을 포함할 수 있다. 또한, 신뢰도 섹션은 전력 시스템에 보안 공격이 진행 중인 확률을 나타내는 공격확률 및 보안상황 경보에 대한 신뢰 점수, 신뢰 점수를 계산하는 노드에 대한 정보를 더 포함할 수 있다. 다만, 상술된 설명은 예시일 뿐, 발명의 구현 형태에 따라 다른 형태의 데이터 포맷이 사용될 수 있음은 물론이다.

[0040] 예를 들어, 신뢰도 섹션의 첫 번째 상위 수준 요소는 전력시스템에서 진행 중인 공격에 대한 백분율 (0과 1 사이)을 나타내는 공격확률로, 복합적인 공격의 백분율을 나타내는 메타 경고에 필요할 수 있다.

[0041] 보안상황 정보수집 및 분석 엔진 모듈(120)은 보안 로그 생성 및 통합 모듈(110)에 의해 추출된 보안 데이터에 기초하여 전력 시스템의 네트워크 및 전력 시스템이 정상 작동 상태에서 실행 중인지 보안위협 상태에서 실행 중인지를 결정할 수 있다. 전력시스템의 네트워크에 있는 보안 시스템 또는 호스트의 상황정보와 네트워크 아키텍처가 분할된 하위 네트워크의 상황정보는 네트워크 및 시스템이 정상 작동 상태에서 실행 중인지 또는 네트워크에서 실행 중인지를 결정하는 요소일 수 있다.

[0042] 전력 시스템 내부 동작이 보안 공격으로 인해 시스템 대기 시간이 갑자기 증가하거나 SSH 로그인 시도 실패 횟수가 실제로 높은 경우, 비정상적으로 동작할 수 있다. 보안 상황정보는 시스템 또는 네트워크가 실제로 공격 또는 손상되고 있을 때, 대응 조치 또는 대응이 효과적으로 적용되었는지를 확인할 수 있다.

- [0043] 보안상황 인식 서비스에서 시스템 및 네트워크 보안상황 분석 엔진은 새로운 침입이 감지되고, 새로운 침입 경고를 받을 때마다 실시간으로 보안 상황정보를 캡처하고 분석하도록 구현될 수 있다. 두 모듈은 모두 분석된 각 지표에서 비정상적인 수준을 계산할 수 있다.
- [0044] 네트워크 보안 상황정보는 전력 시스템 내 서버 네트워크의 트래픽에 대한 스냅샷을 생성하고, 현재 시간 및 날짜, 프로토콜 유형, IP 주소, 포트, IP 대상 주소, 대상 포트, 트래픽 매개 변수, 수신 및 전송된 바이트 등으로 구성될 수 있다. 보안상황 분석 엔진은 이전 스냅샷 정보와 비교하여 네트워크 이상 매개 변수를 계산할 수 있다.
- [0045] 시스템 보안 상황정보는 전력 시스템 내 각종 보안 시스템의 로그 데이터 분석 결과와 활성 프로세스 수, CPU 사용량, 서버 디스크의 여유 공간, CPU 대기 시간, 기록된 사용자 수, 보안 공격 시 구성요소의 여러 시스템 매개 변수 값의 스냅샷, SSH(Secure Shell) 실패 로그인 및 좀비 프로세스 개수 등 시스템 상태 정보로 구성될 수 있다.
- [0046] 보안상황 추론 레이어 모듈(130)은 전력 시스템의 네트워크 및 전력 시스템이 보안위협 상태에서 실행 중인 것으로 결정된 경우, 온톨로지 추론기술을 적용하여 전력시스템의 보안상황 정보를 수집하고, 분석하여 전력시스템의 보안상황 인식서비스를 제공할 수 있다. 이를 위해 보안상황 추론 레이어 모듈(130)은 추론 엔진(Inference Engine)과 온톨로지 저장소(Ontology Repository)로 구성될 수 있다. 트리플 번역기(Triple Translator), 쿼리 핸들러(QueryHandler), 리즈너(Reasoner)는 추론 엔진에 속해 있고, 온톨로지 저장소와 연동될 수 있다.
- [0047] 전력시스템에서 보안 공격이 증가하고, 공격 기술이 정교해짐에 따라 이에 대한 대응을 위해서는 공격탐지 및 대응 프로세스가 자동화될 수 있다. 보안상황 인식 서비스는 가능한 최상의 방어를 제공하기 위해서는 침입에 대해 가장 적절한 대응 방안을 추론할 수 있는 지능형 통합 접근제어 서비스가 필수 요소이다.
- [0048] 전력시스템 내 보안상황 정보를 기반으로 하는 온톨로지는 도 4 및 도 5와 같이 작성될 수 있다.
- [0049] 보안상황 추론 레이어 모듈(130)은 전력시스템 내 각종 보안시스템의 로그 구조 분석을 통하여 보안상황 정보를 획득한 후, 온톨로지의 규칙기반 추론 엔진에 의한 추론을 적용하여, 전력시스템 보안상황 인식서비스를 제공할 수 있다. 보안상황 추론 레이어 모듈(130)은 온톨로지의 사용을 통해, 하위수준의 정보로부터 상위수준의 정보를 추출하며, 정보들을 일반화하고 정보들 사이의 관계를 정의할 수 있다.
- [0050] 보안상황 추론 레이어 모듈(130)은 구성요소를 정의하고 이들 간의 관계를 정의하여야만 명확한 정보를 표현할 수 있다. 따라서, 보안상황 추론 레이어 모듈(130)은 구성요소 간의 관계를 OWL의 속성(Property)으로 정의하여 표현할 수 있다. 즉, OWL의 속성은 관계를 의미한다. 속성의 표현은 Object Properties와 Datatype Properties로 구분되며 Object Properties는 두 Individual 사이의 관계이고, Datatype Properties는 Individual들과 DataValue들 사이의 관계를 표현할 수 있다.
- [0051] 보안상황 추론 레이어 모듈(130)은 도 6에 도시된 바와 같이, 보안상황 정보에서 수집된 침입탐지시스템 정보를 IntrusionDetectionSystem Class로 정의하고, Object Properties로 hasIntrusionTrust, hasIntrusionType, hasNodeLocation, generates 등으로 정의할 수 있다.
- [0052] 또한, 보안상황 추론 레이어 모듈(130)은 intrusionAlertCreateTime, intrusionAlertReliability, intrusionCompletion, intrusionDescription, intrusionDetectionTime 등 요소가 갖는 고유의 데이터를 표현하는 속성이므로 Datatype Properties로 정의할 수 있다.
- [0053] 보안상황 추론 레이어 모듈(130)은 설계한 보안상황 분석 엔진을 이용하여 공격 상태를 감지하기 위하여 공격 전후의 보안상황 정보를 기반으로 공격단계, 침투단계, 수집단계에 대한 상황인지 추론을 위한 SWRL 언어로 추론 규칙을 설계할 수 있다. 여기서, 공격단계는 공격자가 바이러스를 침투시키는 단계이다.
- [0054] 보안상황 추론 레이어 모듈(130)은 공격목표를 지정하고, 목표에 대한 공격 행위를 선택하여, 추론 규칙을 통해 공격단계인지 확인할 수 있다. 공격단계 탐지를 위한 추론 규칙은 예컨대, 도 7에 도시된 바와 같다.
- [0055] 침투단계는 Backdoor 단계와 Movement 단계로 나누어질 수 있다. 공격단계를 통해 바이러스가 침투되면, 침투단계는 침투된 바이러스를 이용하여 직접 시스템을 장악해나가는 단계이다. 개인의 PC를 공격자는 장악하고, 해당 PC를 이용하여 공격자는 자신이 시스템을 계속 사용할 수 있도록 통로를 만들며 PC를 제어할 수 있다.
- [0056] Movement 단계에서는 공격자가 개인의 PC를 이용하여 상위 목표인 기업 서버로 들어가기 위한 공격을 시도하며

서버로 침투할 수 있다. 침투단계 탐지를 위한 추론 규칙은 도 8에 도시된 바와 같다.

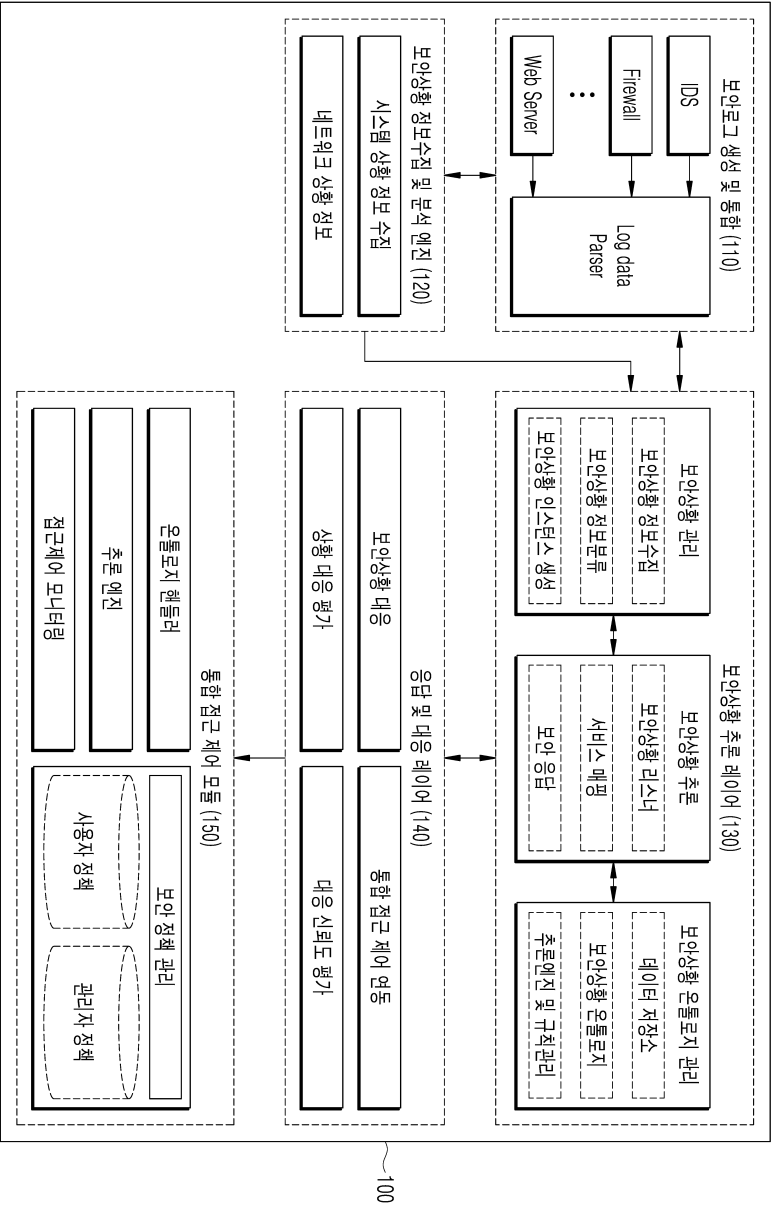
- [0057] 수집단계의 Data Gathering 단계는 공격자가 서버에 접근하고, 마지막 목적을 실행하는 단계이다. 이 단계에서는 공격자가 기업의 기밀정보를 유출하거나, 기업에 피해를 주기 위해 시스템을 파괴하는 단계이다. 수집단계 탐지를 위한 추론 규칙은 도 9에 도시된 바와 같다.
- [0058] 보안상황 온톨로지를 이용한 보안상황 추론은 전력시스템의 보안침입에 대한 최적의 응답을 추론하는 역할을 한다. 시스템 관리자가 정의한 보안정책, 응답, 보안상황 정보 및 침입 경보에 대한 정보를 나타내는 온톨로지 인스턴스를 고려하여 추론 엔진은 특정 침입에 대한 최적의 대응을 결정하기 위한 추론 프로세스를 실행할 수 있다.
- [0059] 보안상황 추론 모듈은 공격탐지에 대한 평가 모듈을 호출하고, Jena 라이브러리를 사용하여 보안상황 온톨로지 에서 추론된 보안상황 정보를 업데이트하고, 응답 레이어에서 처리된 새로운 상황 결과를 업데이트할 수 있다.
- [0060] 응답 및 대응 레이어 모듈(140)은 보안상황 인식 서비스에서 최적의 공격 대응 방안을 추론하고, 추론의 결과에 대한 피드백을 생성하고, 보안 공격에 대한 경고 발생시킨 보안 시스템의 신뢰도를 평가할 수 있다.
- [0061] 지능형 통합 접근제어 모듈(150)은 보안 데이터에 기초한 사용자 인증, 전력 시스템으로의 접근제어 및 보안상황 정보 중 적어도 하나를 관리할 수 있다. 보안상황 접근제어 온톨로지 핸들러는 사용자가 접근하려는 전력 리소스의 권한 서비스로부터 데이터 처리를 통하여 분석한 보안상황 정보를 저장하는 보안상황 접근제어 온톨로지를 관리할 수 있다. 보안정책 관리 모듈은 전력시스템에 접근하려는 주체에 대한 신원확인파 주체의 보안상황 정보를 관리 및 처리할 수 있다. 지능형 접근제어 동작 시나리오는 도 10에 도시된 바와 같다.
- [0063] 본 발명의 명세서(특히 특허청구범위에서)에서 "상기"의 용어 및 이와 유사한 지시 용어의 사용은 단수 및 복수 모두에 해당하는 것일 수 있다. 또한, 본 발명에서 범위(range)를 기재한 경우 상기 범위에 속하는 개별적인 값을 적용한 발명을 포함하는 것으로서(이에 반하는 기재가 없다면), 발명의 상세한 설명에 상기 범위를 구성하는 각 개별적인 값을 기재한 것과 같다.
- [0064] 본 발명에 따른 방법을 구성하는 단계들에 대하여 명백하게 순서를 기재하거나 반하는 기재가 없다면, 상기 단계들은 적당한 순서로 행해질 수 있다. 반드시 상기 단계들의 기재 순서에 따라 본 발명이 한정되는 것은 아니다. 본 발명에서 모든 예들 또는 예시적인 용어(예들 들어, 등등)의 사용은 단순히 본 발명을 상세히 설명하기 위한 것으로서 특허청구범위에 의해 한정되지 않는 이상 상기 예들 또는 예시적인 용어로 인해 본 발명의 범위가 한정되는 것은 아니다. 또한, 당업자는 다양한 수정, 조합 및 변경이 부가된 특허청구범위 또는 그 균등물의 범주 내에서 설계 조건 및 팩터에 따라 구성될 수 있음을 알 수 있다.
- [0065] 따라서, 본 발명의 사상은 상기 설명된 실시 예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 또는 이로부터 등가적으로 변경된 모든 범위는 본 발명의 사상의 범주에 속한다고 할 것이다.

부호의 설명

- [0066] 100: 스마트그리드에서 보안상황 인식을 위한 지능형 접근제어 장치
- 110: 보안 로그 생성 및 통합 모듈
- 120: 보안상황 정보수집 및 분석 엔진 모듈
- 130: 보안상황 추론 레이어 모듈
- 140: 응답 및 대응 레이어 모듈
- 150: 지능형 통합 접근제어 모듈

도면

도면1

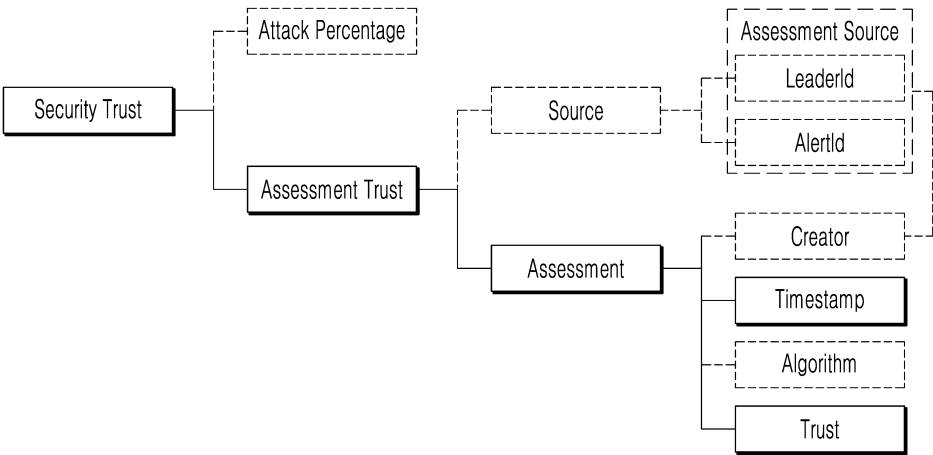


도면2

클래스	결합성	형식	설명
Analyzer	exactly one		경고를 생성한 분석기에 대한 식별 정보
CreateTime	exactly one	DATETIME	경고가 생성된 시간
Classification	exactly one		경고의 이름 또는 관리기로 하여금 해당 내용이 무엇인 지 알게끔 하는 정보
DetectTime	zero or one	DATETIME	경고를 발생하는 이벤트가 검출된 시간 하나 이상의 이벤트가 관계된 경우, 첫 번째 이벤트가 검출된 시간 CreateTime 클래스와 다른 값을 가질 수 있음
AnalyzerTime	zero or one	DATETIME	분석기의 현재 시간
Source	zero or one		경고가 발생한 이벤트의 원천
Target	zero or one		경고가 발생한 이벤트의 대상
Assessment	zero or one		이벤트의 영향, 분석기의 대응 조치, 분석기의 평가
AdditionalData	zero or one		데이터 모델에 적합하지 않은 분석기에 의해 생성되는 추가적인 정보
RawPacket	zero or one	BYTE[]	경고를 발생한 패킷 정보

공격 클래스 요소

도면3



IDMEF에서 신뢰도 섹션 확장 설계

도면4



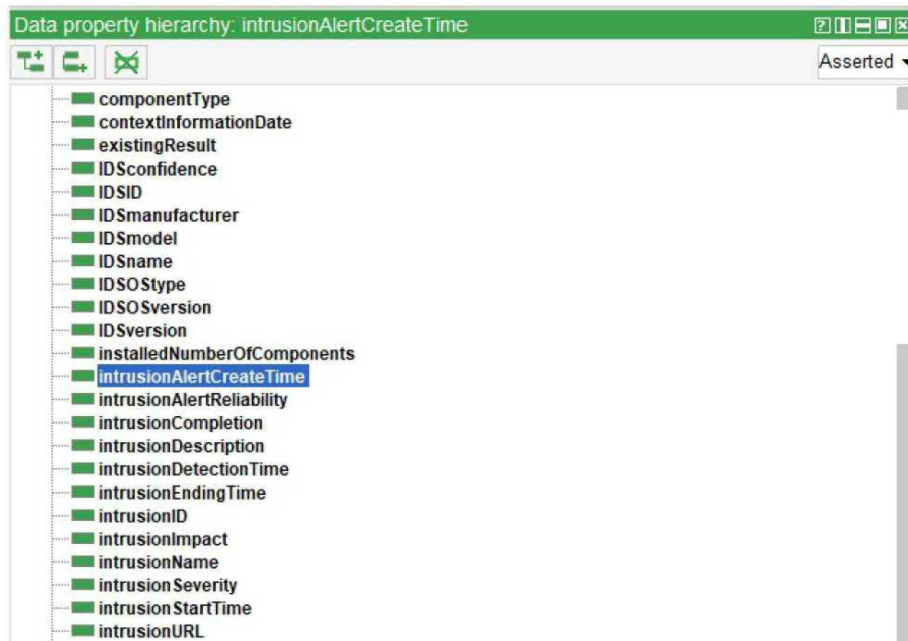
보안상황 공격 분류 클래스

도면5



보안상황 공격 개체 속성

도면6



침입 탐지 시스템 클래스의 데이터 속성

도면7

공격 추론 대상	추론 규칙
이메일 공격	(?T behaviour Spearphishing_mail) ^ (Spearphishing resultIn RemoteAccess) ^ (RemoteAccess resultIn System_Control) ⇒ (?T step VariousAttack)
웹 사이트 공격	(?T behaviour InfetedWebsite) ^ (InfetedWebsite resultIn RemoteAccess) ^ (RemoteAccess resultIn System_Control) ⇒ (?T step VariousAttack)

보안상황 정보 온톨로지를 이용한 APT 공격단계 추론 규칙 예

도면8

공격 추론 대상	추론 규칙
네트워크 트래픽 증가	(?T behaviour RemoteAccess) ^ (RemoteAccess resultIn System_Control) ^ (System_Control resultIn Networktraffic_increase) ⇒ (?T step Backdoor)
서버 공격	(?T behaviour DenialOfService) ^ (DenialOfService resultIn LossOfIntegrity) ^ (LossOfIntegrity resultIn MaliciousCodeExecution) ⇒ (?T step Movement)

보안상황 정보 온톨로지를 이용한 APT 침투단계 추론규칙 예

도면9

공격 추론 대상	추론 규칙
서버 접속 후 정보 유출	$(?T \text{ behaviour Server_Connect}) \wedge (\text{Server_Connect resultIn Information_Leakage}) \Rightarrow (?T \text{ step Data Gathering})$
서버 접속 후 시스템 파괴	$(?T \text{ behaviour Server_Connect}) \wedge (\text{Server_Connect resultIn System_Destruction}) \Rightarrow (?T \text{ step Data Gathering})$

보안상황 정보 온톨로지를 이용한 APT 수집단계 추론 규칙 예

도면10

