

발명의 설명

발명의 명칭: 공격표면 정보 기반 의 디셉션 정보 생성 시스템 및 방법

기술분야

- [1] 본 발명은 공격표면 정보 기반의 디셉션(Deception) 정보 생성 시스템 및 방법에 관한 것으로, 선박을 공격하는 사이버 공격자에 대해 공격자를 기만하여 실제 선박 내부 시스템으로 위장하여 공격 초기 단계에서 공격 징후 식별하여 초기 대응을 하여 선박을 지키기 위한 기술에 관한 것이다.

배경기술

- [2] 종래에는 사이버 위협에 대하여, 기만(deception) 기술 기반의 사이버 공격 유인하는 것으로 사이버 공격자를 기만하여 공격을 유인하고 감시를 위한 공격자 기만 프레임워크와 모듈을 개발하여 사이버 공격 준비 단계에서의 이상 탐지로 인하여 피해 확산을 차단하고, 기만기술에 탐지된 로그를 타 보안장비와 연동을 통해 탐지율을 향상시켰다.
- [3] 또한, ICT 기반의 자율운항선박, 스마트십, 무인선 건조가 급격히 증가하고, 육상과 해상 선박의 연결성이 높아지면서 선박 사이버 위협이 증가하고 있으나 육상과 같은 다양한 보안 시스템 구축 운용이 제한되며, 선체 내부의 모든 보안 로그를 육상으로 전송 시 위성통신비용이 과다 발생하는 문제점이 있었다.
- [4] 또한, 도 1에 도시된 바와 같이, 디셉션 관련 기술은 모니터링 장치 또는 정상적인 장치로 위장한 미끼 시스템을 네트워크 앞에 위치시키고 해당 장치에서 수신된 패킷이 종래에 사용되는 IP인 경우 정상, 비사용 IP인 경우 디코이(Decoy)에 이전트로 전송하는 것으로 선체 내부의 통신 경로는 IEEE6112-450/460 환경으로 제한적이므로 가상화 기반으로 많은 수의 취약한 시스템을 가동하여 유인되는 공격자를 분석하다 보니 선박에 탑재되어야 하는 리소스(시스템, VM, IP 등)가 과다하게 필요하고, 제한된 선박 시스템, 네트워크, 인적자원 환경에서는 어려움이 있었다.
- [5] 관련선행문헌으로는 대한민국 공개특허 제10-2020-0055403호(2020.05.21.)이 공개되어 있다.

발명의 내용

기술적 과제

- [6] 본 발명의 목적은 스마트십, 자율운항선박 등 ICT 기반 선박 건조가 증가함에 따라 새로운 환경에서의 사이버 위협 탐지와 방어 기술을 확보할 수 있는 공격표면 정보 기반의 디셉션 정보 생성 시스템 및 방법을 제공하는 것을 목적으로 한다.
- [7] 본 발명의 다른 목적은 공격자를 기만하여 실제 선박 내부 시스템으로 위장하여 공격 초기 단계에서 공격 징후 식별이 가능하도록 하여 시스템 피해 발생 전

에 대처할 수 있는 공격표면 정보 기반의 디셉션 정보 생성 시스템 및 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [8] 상기한 목적을 달성하기 위한 본 발명의 일측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템은, 공격표면 정보 기반의 디셉션 정보 생성 시스템은 선박을 공격하는 사이버 공격자에 대하여 공격자를 기만하는 기만 단말 및 실제 선박 내부 시스템으로 위장하여 사이버 공격을 유인하여 정보를 분석하는 유인 단말을 포함하되, 상기 기만 단말은, 유인 정보를 생성하는 유인정보 생성부와, 유인 단말에 접근한 사용자 혹은 시스템, 장치로부터 정상 사용자 인지 악의적 사용자 인지를 판단하는 유인 정보 판단부 및, 유인된 사용자 혹은 시스템, 장치가 악의적 사용자인 경우 차단 혹은 알람 이벤트를 송신하는 유인 정보 조치부를 포함하며; 상기 유인 단말은, 유인 단말에 최초 접근하는 패킷을 수집하는 유인자 정보 수집부와, 유인 단말에 인입된 패킷을 분석하는 유인자 정보 분석부 및, 기만 단말의 유인 정보 생성부에서 생성된 유인 정보를 통해 생성된 유인 에이전트가 동작되도록 하는 유인부를 포함하며; 상기 기만 단말에서 인입된 패킷 정보와 유인된 접속자의 입력정보 등의 수신정보를 기반으로 유인자의 위험도를 판단하여, 설정값 이상인 경우 공격자로 판단하고 알람을 통해 조치할 수 있도록 한다.
- [9] 또한, 본 발명의 일측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 상기 기만 단말의 유인 정보 생성부는, 선박 해양 위성통신 시스템의 웹 페이지와 구성 파일, 동적 항해 정보, 시스템의 하드웨어 정보(MAC)를 생성하는 것을 특징으로 한다.
- [10] 또한, 본 발명의 일측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 상기 기만 단말의 유인 정보 판단부는, 인입된 패킷과 유인된 접속자의 입력정보 등 수신정보를 기반으로 유인자의 공격자 여부를 위험도 점수를 기반으로 판단하는 것을 특징으로 한다.
- [11] 또한, 본 발명의 일측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 상기 기만 단말의 유인 정보 조치부는, 위험도가 일정 수준 이상으로 계산된 경우 공격자로 판단하고, 기만 시스템이 사용자에게 비상벨, 메시지 등으로 알람을 표시하거나, 선박 단말장치에 표시하거나, 선박 알람 모니터링 시스템의 HMI에 메시지를 표출하는 것을 특징으로 한다.
- [12] 또한, 본 발명의 일측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 상기 유인 단말의 유인 정보 분석부는, 유인 단말에 인입된 패킷의 신호를 분류하고, 분류된 신호에서 메시지의 값을 정의하여 추출하고, 추출된 메시지 값에서 유인자 정보를 추출할 수 있다.
- [13] 또한, 본 발명의 일측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 상기 유인 단말의 유인부는, 기만 단말의 유인 정보 생성부로부터 생성된

선박 내 기자재 시스템의 특징을 가지는 프로그램, 운영체제, 시스템 정보로 생성된 유인 에이전트가 동작하도록 한다.

- [14] 본 발명의 다른 측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 방법은, 공격표면 정보 기반의 디셉션 정보 생성 시스템은 선박을 공격하는 사이버 공격자에 대하여 공격자를 기만하는 기만 단말, 및 실제 선박 내부 시스템으로 위장하여 사이버 공격을 유인하여 정보를 분석하는 유인 단말을 포함하되, 상기 기만 단말의 유인정보 생성부에서 유인 정보를 생성하는 유인 정보 생성 단계; 상기 유인 정보 생성 단계에서 생성된 유인정보를 수신하고, 유인 단말에 최초 접근하는 패킷을 유인 정보 수집부에서 수집하는 유인자 정보 수집 단계; 상기 유인자 정보 수집 단계에서 수집된 유인자 정보와 패킷을 분석하는 유인자 정보 분석 단계; 기만 단말의 유인 정보 생성부에서 생성된 유인 정보를 통해 생성된 유인 에이전트가 유인부에서 동작되도록 하는 유인 단계; 상기 유인 단계에서 유인 단말에 접근한 사용자 혹은 시스템, 장치로부터 정상 사용자 인지 악의적 사용자 인지를 판단하는 유인 정보 판단 단계; 상기 유인 정보 판단 단계를 통해 유인된 사용자 혹은 시스템, 장치가 악의적 사용자인 경우 차단 혹은 알람 이벤트를 유인 정보 조치부에서 송신하는 조치 단계를 포함할 수 있다.
- [15] 또한, 본 발명의 다른 측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 방법에서, 상기 유인 정보 생성 단계는, 선박 해양 위성통신 시스템의 웹 페이지와 구성 파일, 동적 항해 정보, 시스템의 하드웨어 정보(MAC)를 생성하는 것을 특징으로 한다.
- [16] 또한, 본 발명의 다른 측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 방법에서, 상기 유인 정보 판단 단계는, 인입된 패킷과 유인된 접속자의 입력정보 등 수신정보를 기반으로 유인자의 공격자 여부를 위험도 점수를 기반으로 판단하는 것을 특징으로 한다.
- [17] 또한, 본 발명의 다른 측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 방법에서, 상기 조치 단계는, 위험도가 일정 수준 이상으로 계산된 경우 공격자로 판단하고, 기만 시스템이 사용자에게 비상벨, 메시지 등으로 알람을 표시하거나, 선박 단말장치에 표시하거나, 선박 알람 모니터링 시스템의 HMI에 메시지를 표출하는 것을 특징으로 한다.
- [18] 또한, 본 발명의 다른 측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 방법에서, 상기 유인자 정보 분석 단계는, 유인 단말에 인입된 패킷의 신호를 분류하고, 분류된 신호에서 메시지의 값을 정의하여 추출하고, 추출된 메시지 값에서 유인자 정보를 추출할 수 있다.
- [19] 또한, 본 발명의 다른 측면에 따른 공격표면 정보 기반의 디셉션 정보 생성 방법에서, 상기 유인 단계는, 기만 단말의 유인 정보 생성부로부터 생성된 선박 내 기자재 시스템의 특징을 가지는 프로그램, 운영체제, 시스템 정보로 생성된 유인 에이전트가 동작하도록 한다.

발명의 효과

- [20] 본 발명에 따르면, 스마트집, 자율운항선박 등 ICT 기반 선박 건조가 증가함에 따라 새로운 환경에서의 사이버 위협 탐지와 방어 기술을 확보할 수 있는 효과를 갖는다.
- [21] 또한 본 발명에 따르면, 공격자를 기만하여 실제 선박 내부 시스템으로 위장하여 공격 초기 단계에서 공격 징후 식별이 가능하도록 하여 시스템 피해 발생 전에 대처할 수 있는 효과를 갖는다.

도면의 간단한 설명

- [22] 도 1은 종래의 사이버 위협에 대한 기만(deception) 기술을 나타내는 도면이다.
- [23] 도 2는 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템의 구성을 나타내는 도면이다.
- [24] 도 3은 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 유인자 정보 분석부에서 수행되는 과정을 나타내는 도면이다.
- [25] 도 4는 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 유인자 정보 분석부의 세부 데이터를 나타내는 도면이다.
- [26] 도 5는 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 유인자 정보 판단부에서 수행되는 과정을 나타내는 도면이다.
- [27] 도 6은 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템에서 유인자 정보 조치부에서 수행되는 알람 표시 실시예를 나타내는 도면이다.

발명의 실시를 위한 형태

- [28] 본 발명의 목적과 기술적 구성 및 그에 따른 작용 및 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 상세한 설명에 의해 보다 명확하게 이해될 것이다.
- [29] 본 명세서에서 사용되는 용어는 단지 특정한 실시예를 설명하기 위해 사용되는 것으로 본 발명을 한정하려는 의도가 아니다. 예컨대, 본 명세서에서 사용되는 '구성된다' 또는 '포함한다' 등의 용어는 발명에 기재된 여러 구성요소들 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성요소들 또는 일부 단계들을 포함하지 않거나 또는 추가적인 구성요소들 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다.
- [30] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써 본 발명을 상세히 설명한다. 이하에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의해 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 이 분야의 통상의 기술자에게 다양한 응용을 가질 수 있음은 당연하다.

- [31] 도 2 내지 도 6을 참조하면, 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템(100)은 유인 정보를 생성하는 유인정보 생성부(111)와, 유인 단말에 접근한 사용자 혹은 시스템, 장치로부터 정상 사용자 인지 악의적 사용자 인지를 판단하는 유인정보 판단부(112) 및 유인된 사용자 혹은 시스템, 장치가 악의적 사용자인 경우 차단 혹은 알람 이벤트를 송신하는 유인 정보 조치부(113)를 포함하는 기만 단말(110)과, 유인 단말에 최초 접근하는 패킷을 수집하는 유인자 정보 수집부(121)와 유인 단말에 인입된 패킷을 분석하는 유인자 정보 분석부(122) 및 기만 단말의 유인 정보 생성부에서 생성된 정보를 통해 생성된 유인 에이전트가 동작되도록 하는 유인부(113)을 포함할 수 있다.
- [32] 이때, 공격표면 정보 기반의 디셉션 정보 생성 시스템(100)은 선박의 802.1x 환경을 고려한 격리 수단을 고려한 것으로 신조 선박에 탑재되는 사이버보안 기술로 802.1x protocol mandatory을 적용하였다.
- [33] 또한 무선 환경에서 사용되는 프로토콜(protocol)이나 장비 인증 방식 대안으로 적용할 수 있으며, 시스템과의 입증(prove) 연동을 통한 인증 해제(deauthentication)/분리(disassociation)로 차단 가능하다.
- [34] 본 발명에 따른 공격표면 정보 기반의 디셉션 정보 생성 시스템(100)의 기만 단말(110)의 유인정보 생성부(111)는 사이버 공격자가 선박 내부 시스템으로 오인하도록 유도하는 선박 내 주요 시스템의 정보를 생성한다.
- [35] 또한, 시스템의 주요 정보는 선박 항해, 통신, 제어, 추진, 전력 시스템의 운영체제, 프로그램, 네트워크의 특징을 갖도록 구성될 수 있다.
- [36] 또한, 항해 정보(Heading, Speed, GPS, 쓰로틀, 온도, 압력 등)와 각 시스템의 제조사, 제품명, 하드웨어 정보(MAC)등을 포함할 수 있다.
- [37] 또한, 유인 정보 생성부(111)에서 생성된 정보는 유인 단말에 주입될 수 있다.
- [38] 즉, 유인 단말(120)의 유인자 정보 수집부(121)에서는 유인 단말(120)에 최초 접근하는 패킷을 수집할 수 있으며, 인터페이스는 산업계 표준인 RS-232, RS-422, Modbus TCP Master/Slave로 구성될 수 있다.
- [39] 또한, 유인자 정보 분석부(122)에서는 유인 단말(120)에 인입된 패킷을 분석한다. TCP 패킷에서 일반적으로 알려진 HTTP, FTP, SSH 등의 프로토콜과 TCP 패킷에 포함된 MODBUS, NMEA, PLC, CAN을 분류한다.
- [40] 도 3 및 도 4에 도시된 바와 같이, 유인자 정보 분석부(122)는 인입된 패킷(S210)으로부터 신호를 분류하는 신호 분류 단계(S220)와, 신호 분류 단계(S220)를 통해 분류된 신호에서 메시지의 값을 추출하는 패킷 정의 단계(S230)와, 패킷 정의 단계(S230)에서 추출된 메시지 값을 통해 패킷 정보를 추출하여 유인자 정보를 확인하는 패킷 추출 단계(S240)를 포함한다.
- [41] 보다 구체적으로는, 유인자 정보 분석부(122)에서는 유인 단말(120)에 인입된 패킷(S210)으로부터 신호를 분류(S220)한다.
- [42] 이때 신호를 분류하는 신호 분류 단계(S220)는 인입된 패킷으로부터 normal tcp 패킷과 제어용 단말장치에서 tcp 패킷으로 전송된 패킷인지 분류한다.

- [43] 이어서 패킷 정의 단계(S230)에서는 분류된 신호에서 메시지의 값을 추출한다.
- [44] 예를 들어 MODBUS-TCP인 경우 메시지의 값은 산업계 표준인 RS-485/Modbus-RTU로부터 정의된다.
- [45] 패킷 추출 단계(S240)에서는 IP address, Port, Unit ID, Protocol, Slave Address, Baud Rate 등을 확인한다.
- [46] 유인 단말(120)의 유인부(123)에서는 기만 단말(110)의 유인 정보 생성부(111)로부터 생성된 선박 내 기자재 시스템의 특징을 가지는 프로그램, 운영체제, 시스템 정보로 생성된 유인 에이전트가 동작한다.
- [47] 유인 에이전트는 HTTP, FTP, SSH, SFTP, TELNET, MODBUS, PLC, CAN, NMEA 프로토콜과 이에 해당하는 포트 정보와 MAC 정보로 동작한다.
- [48] 예를 들어, 유인 정보 생성부(111)에서 선박 해양위성통신 시스템의 유인정보가 생성된 경우, 이를 구성하는 웹 페이지와 구성 파일, 동적 항해 정보, 시스템의 하드웨어 정보(MAC)가 생성된다.
- [49] 동적 항해 정보는 선박의 현재 위치(GPS position), heading, knot) 등 상세 정보로 구성될 수 있다.
- [50] 또한, 유인 정보 생성부(111)에서 선박 알람 모니터링 시스템(AMS)로 유인정보가 생성된 경우, 이를 구성하는 하드웨어 정보(MAC), 열린 포트의 정보, 가동중인 서비스 정보로 구성될 수 있다.
- [51] 유인 정보 판단부(112)는 인입된 패킷과 유인된 접속자의 입력정보 등 수신정보를 기반으로 유인자의 공격자 여부를 위험도 점수를 기반으로 판단한다.
- [52] 즉, 도 5에 도시된 바와 같이, 수신정보를 기반으로 등록된 CBS IP(Computer Based System Internet Protocol)인지 여부를 확인하여, 등록된 경우 위험도 점수를 0점, 등록되지 않은 경우 위험도 점수 3점을 부여한다.
- [53] 이어서, 등록된 CBS IP의 Port인지 여부를 확인하여, 등록된 경우 위험도 점수를 0점, 등록되지 않은 경우 위험도 점수 3점을 부여한다.
- [54] 이어서, 등록된 CBS MAC인지 여부를 확인하여, 등록된 경우 위험도 점수를 0점, 등록되지 않은 경우 위험도 점수 3점을 부여한다.
- [55] 즉, 등록된 경우는 위험도 점수가 상승하지 않고 등록되지 않은 경우 위험도 점수가 누적되어 상승할 수 있다.
- [56] 이어서, 등록된 출발지 IP의 소유자는 누구인지 여부를 확인하여, 장치(Device)인 경우 위험도 점수를 0점, 승무원(crew)인 경우 위험도 점수 3점을 부여한다.
- [57] 이어서, 소유자 권한 판단하여, LOCAL인 경우 위험도 점수를 1점, REMOTE인 경우 위험도 점수 3점을 부여한다.
- [58] 이어서, 등록 IP 소유자 위치 Hop 정보를 확인하여 같은 경우 위험도 점수를 1점, 다른 경우 위험도 점수 3점을 부여한다.
- [59] 이어서, 요청 횟수를 확인하여 1회인 경우 위험도 점수를 1점, n회 이상인 경우 위험도 점수 3점을 부여한다.

- [60] 이어서, 입력 정보의 실패 횟수를 확인하여 1회인 경우 위험도 점수를 1점, n회 이상인 경우 위험도 점수 3점을 부여한다.
- [61] 이어서 총 합계 점수를 바탕으로 위험도를 판단하고 설정값 이상인 경우 공격자로 판단할 수 있다.
- [62] 유인 정보 조치부(113)은 위험도가 일정 수준 이상으로 계산된 경우 공격자로 판단하고, 기만 시스템이 사용자(선원, 육상 근무자)에게 비상벨, 메시지 등으로 알람을 표시하거나, 선박 단말장치에 표시하거나, 선박 알람 모니터링 시스템(AMS)의 HMI에 메시지를 표출할 수 있다.
- [63] 표출되는 메시지는 도 6에 도시된 바와 같이, 탐지된 Source IP와 등록된 CBS Inventory 정보를 비교하여 해당 IP가 사용하고 있는 Deck, Room, IP, MAC, User/System 정보를 표시한다. 이로써 육상/승선 근무자가 원격 조치 또는 현장 조치할 수 있도록 한다.
- [64] 따라서 본 발명에 따르면, 스마트십, 자율운항선박 등 ICT 기반 선박 건조가 증가함에 따라 새로운 환경에서의 사이버 위협 탐지와 방어 기술을 확보할 수 있는 효과를 갖는다.
- [65] 또한 본 발명에 따르면, 공격자를 기만하여 실제 선박 내부 시스템으로 위장하여 공격 초기 단계에서 공격 징후 식별이 가능하도록 하여 시스템 피해 발생 전에 대처할 수 있는 효과를 갖는다.
- [66] 이상 설명된 본 발명에 따른 실시예는 다양한 컴퓨터 구성요소를 통하여 실행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 판독 가능한 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium) 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위하여 하나 이상의 소프트웨어 모듈로 변경될 수 있으며 그 역도 마찬가지이다.
- [67] 이상에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의하여 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 본 발명의 사상 및 범위를 벗어나지 않는 범위 내에서 다양하게 수정 및 변형될 수 있음은 이 기술의 분야에서 통상의

지식을 가진 자에게 자명하다. 따라서 그러한 수정예 또는 변형예들은 본 발명의 특허청구범위에 속한다 하여야 할 것이다.

서열목록

- [68] 100: 공격표면 정보 기반의 디셉션 정보 생성 시스템
- [69] 110: 기판 단말
- [70] 111: 유인 정보 생성부
- [71] 112: 유인 정보 판단부
- [72] 113: 유인 정보 조치부
- [73] 120: 유인 단말
- [74] 121: 유인자 정보 수집부
- [75] 122: 유인자 정보 분석부
- [76] 123: 유인부

청구범위

- [청구항 1] 공격표면 정보 기반의 디셉션 정보 생성 시스템은 선박을 공격하는 사이버 공격자에 대하여 공격자를 기만하는 기만 단말 및 실제 선박 내부 시스템으로 위장하여 사이버 공격을 유인하여 정보를 분석하는 유인 단말을 포함하되,
- 상기 기만 단말은, 유인 정보를 생성하는 유인정보 생성부와, 유인 단말에 접근한 사용자 혹은 시스템, 장치로부터 정상 사용자 인지 악의적 사용자 인지를 판단하는 유인 정보 판단부 및, 유인된 사용자 혹은 시스템, 장치가 악의적 사용자인 경우 차단 혹은 알람 이벤트를 송신하는 유인 정보 조치부를 포함하며;
- 상기 유인 단말은, 유인 단말에 최초 접근하는 패킷을 수집하는 유인자 정보 수집부와, 유인 단말에 인입된 패킷을 분석하는 유인자 정보 분석부 및, 기만 단말의 유인 정보 생성부에서 생성된 유인 정보를 통해 생성된 유인 에이전트가 동작되도록 하는 유인부를 포함하며;
- 상기 기만 단말에서 인입된 패킷 정보와 유인된 접속자의 입력정보 등의 수신정보를 기반으로 유인자의 위험도를 판단하여, 설정값 이상인 경우 공격자로 판단하고 알람을 통해 조치할 수 있도록 하는, 공격표면 정보 기반의 디셉션 정보 생성 시스템.
- [청구항 2] 청구항 1에 있어서,
- 상기 기만 단말의 유인 정보 생성부는,
- 선박 해양 위성통신 시스템의 웹 페이지와 구성 파일, 동적 항해 정보, 시스템의 하드웨어 정보(MAC)를 생성하는 것을 특징으로 하는, 공격표면 정보 기반의 디셉션 정보 생성 시스템.
- [청구항 3] 청구항 1에 있어서,
- 상기 기만 단말의 유인 정보 판단부는,
- 인입된 패킷과 유인된 접속자의 입력정보 등 수신정보를 기반으로 유인자의 공격자 여부를 위험도 점수를 기반으로 판단하는 것을 특징으로 하는, 공격표면 정보 기반의 디셉션 정보 생성 시스템.
- [청구항 4] 청구항 1에 있어서,
- 상기 기만 단말의 유인 정보 조치부는,
- 위험도가 일정 수준 이상으로 계산된 경우 공격자로 판단하고, 기만 시스템이 사용자에게 비상벨, 메시지 등으로 알람을 표시하거나, 선박 단말장치에 표시하거나, 선박 알람 모니터링 시스템의 HMI에 메시지를 표출하는 것을 특징으로 하는, 공격표면 정보 기반의 디셉션 정보 생성 시스템.
- [청구항 5] 청구항 1에 있어서,
- 상기 유인 단말의 유인 정보 분석부는,

유인 단말에 인입된 패킷의 신호를 분류하고, 분류된 신호에서 메시지의 값을 정의하여 추출하고, 추출된 메시지 값에서 유인자 정보를 추출하는, 공격표면 정보 기반의 디셉션 정보 생성 시스템.

[청구항 6]

청구항 1에 있어서,
상기 유인 단말의 유인부는,
기만 단말의 유인 정보 생성부로부터 생성된 선박 내 기자재 시스템의 특징을 가지는 프로그램, 운영체제, 시스템 정보로 생성된 유인 에이전트가 동작하도록 하는, 공격표면 정보 기반의 디셉션 정보 생성 시스템.

[청구항 7]

공격표면 정보 기반의 디셉션 정보 생성 시스템은 선박을 공격하는 사이버 공격자에 대하여 공격자를 기만하는 기만 단말, 및 실제 선박 내부 시스템으로 위장하여 사이버 공격을 유인하여 정보를 분석하는 유인 단말을 포함하되,
상기 기만 단말의 유인정보 생성부에서 유인 정보를 생성하는 유인 정보 생성 단계;
상기 유인 정보 생성 단계에서 생성된 유인정보를 수신하고, 유인 단말에 최초 접근하는 패킷을 유인 정보 수집부에서 수집하는 유인자 정보 수집 단계;
상기 유인자 정보 수집 단계에서 수집된 유인자 정보와 패킷을 분석하는 유인자 정보 분석 단계;
기만 단말의 유인 정보 생성부에서 생성된 유인 정보를 통해 생성된 유인 에이전트가 유인부에서 동작되도록 하는 유인 단계;
상기 유인 단계에서 유인 단말에 접근한 사용자 혹은 시스템, 장치로부터 정상 사용자 인지 악의적 사용자 인지를 판단하는 유인 정보 판단 단계;
상기 유인 정보 판단 단계를 통해 유인된 사용자 혹은 시스템, 장치가 악의적 사용자인 경우 차단 혹은 알람 이벤트를 유인 정보 조치부에서 송신하는 조치 단계를 포함하는, 공격표면 정보 기반의 디셉션 정보 생성 방법.

[청구항 8]

청구항 7에 있어서,
상기 유인 정보 생성 단계는,
선박 해양 위성통신 시스템의 웹 페이지와 구성 파일, 동적 항해 정보, 시스템의 하드웨어 정보(MAC)를 생성하는 것을 특징으로 하는, 공격표면 정보 기반의 디셉션 정보 생성 방법.

[청구항 9]

청구항 7에 있어서,
상기 유인 정보 판단 단계는,
인입된 패킷과 유인된 접속자의 입력정보 등 수신정보를 기반으로 유인자의 공격자 여부를 위험도 점수를 기반으로 판단하는 것을 특징으로 하는, 공격표면 정보 기반의 디셉션 정보 생성 방법.

[청구항 10]

청구항 7에 있어서,

상기 조치 단계는,

위험도가 일정 수준 이상으로 계산된 경우 공격자로 판단하고, 기만 시스템이 사용자에게 비상벨, 메시지 등으로 알람을 표시하거나, 선박 단말장치에 표시하거나, 선박 알람 모니터링 시스템의 HMI에 메시지를 표출하는 것을 특징으로 하는, 공격표면 정보 기반의 디셉션 정보 생성 방법.

[청구항 11]

청구항 7에 있어서,

상기 유인자 정보 분석 단계는,

유인 단말에 인입된 패킷의 신호를 분류하고, 분류된 신호에서 메시지의 값을 정의하여 추출하고, 추출된 메시지 값에서 유인자 정보를 추출하는, 공격표면 정보 기반의 디셉션 정보 생성 방법.

[청구항 12]

청구항 7에 있어서,

상기 유인 단계는,

기만 단말의 유인 정보 생성부로부터 생성된 선박 내 기자재 시스템의 특징을 가지는 프로그램, 운영체제, 시스템 정보로 생성된 유인 에이전트가 동작하도록 하는, 공격표면 정보 기반의 디셉션 정보 생성 방법.