



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0010315
(43) 공개일자 2025년01월21일

(51) 국제특허분류(Int. Cl.)
G09B 19/00 (2006.01) G06F 13/42 (2006.01)
G09B 9/00 (2006.01) H04L 43/50 (2022.01)
H04L 9/40 (2022.01)
(52) CPC특허분류
G09B 19/0053 (2013.01)
G06F 13/4282 (2013.01)
(21) 출원번호 10-2023-0090375
(22) 출원일자 2023년07월12일
심사청구일자 2023년07월12일

(71) 출원인
건양대학교산학협력단
충청남도 논산시 대학로 121 (내동)
(72) 발명자
김동원
충청남도 논산시 연무읍 안심로 150-22 골든팰리스 102동1602호
(74) 대리인
강정빈, 심찬

전체 청구항 수 : 총 5 항

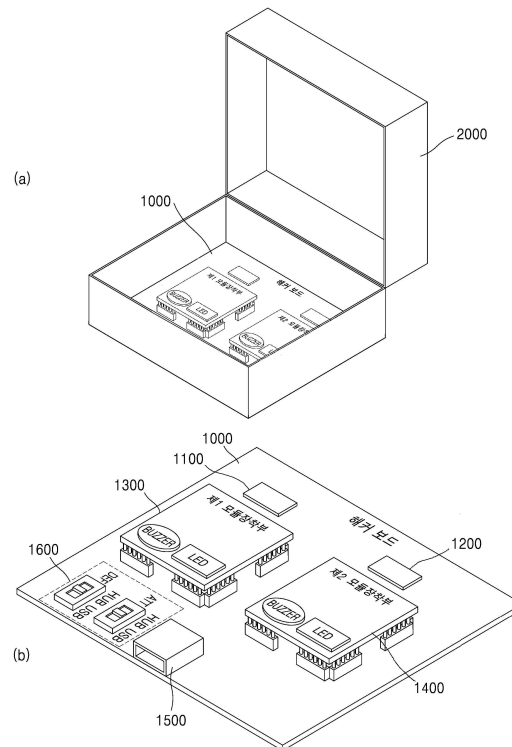
(54) 발명의 명칭 두 개의 MCU를 포함하는 해커보드실습장치

(57) 요약

본 발명은 두 개의 MCU를 포함하는 해커보드실습장치로서, 하나의 케이스에 구비될 수 있는 해커보드에 포함된 제1MCU 및 제1MCU의 성능을 확장시키는 제1모듈장착부와 제2MCU 및 제2MCU의 성능을 확장시키는 제2모듈장착부를 통해 해킹교육에 있어 실습자가 하나의 해커보드실습장치를 이용하여 적외선신호 혹은 UART신호에 대한 모의해킹

(뒷면에 계속)

대표도 - 도1



의 공격시뮬레이션 및 방ersi뮬레이션을 동시에 수행할 수 있는, 두 개의 MCU를 포함하는 해커보드실습장치에 관한 것이다.

또한 본 발명은 하기 연구과제의 결과물에 해당하는 것이다.

[과제번호] 202203670001

[지원기관] 에스알센터

[연구사업명] 산업체공동 연구과제 지원사업

[연구과제명] 기반시설 운영시스템의 생애주기(Life-cycle) 보안모델 연구

[주관기관] 건양대학교 산학협력단

[연구기간] 2022.11.10 ~ 2022.12.10.

(52) CPC특허분류

G09B 9/00 (2013.01)

H04L 43/50 (2022.05)

H04L 63/14 (2013.01)

G06F 2213/0042 (2013.01)

명세서

청구범위

청구항 1

모의해킹에 대한 시뮬레이션을 수행하는 해커보드실습장치로서,

해커보드; 및

케이스;를 포함하고,

상기 해커보드는,

1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 모의해킹에 대한 공격시뮬레이션을 수행하는 제1MCU;

1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 모의해킹에 대한 방어시뮬레이션을 수행하는 제2MCU;

상기 제1MCU와 연결되고, 상기 공격시뮬레이션의 수행여부를 출력하는 부저 혹은 LED를 포함하는 복수의 전자모듈을 포함할 수 있는 제1모듈장착부;

상기 제2MCU와 연결되고, 상기 방어시뮬레이션의 수행여부를 출력하는 부저 혹은 LED를 포함하는 복수의 전자모듈을 포함할 수 있는 제2모듈장착부;

상기 제1MCU 및 상기 제2MCU를 외부 컴퓨팅장치와 연결하고, 상기 외부 컴퓨팅장치로부터 공격코드 및 방어코드를 수신하는 USB커넥터; 및

상기 제1MCU 및 상기 제2MCU에 대한 상기 USB커넥터의 연결을 제어하는 USB스위치모듈;을 포함하고,

상기 해커보드는 하나의 상기 케이스 내부에 설치될 수 있는, 해커보드실습장치.

청구항 2

청구항 1에 있어서,

상기 해커보드실습장치는 적외선스니핑시나리오 혹은 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행하고,

상기 제1MCU는 공격자MCU로써, 상기 USB커넥터를 통해 상기 외부 컴퓨팅장치로부터 해당 시나리오에 대한 공격코드가 입력되어 공격시뮬레이션을 수행하고,

상기 제2MCU는 방어자MCU로써, 상기 USB커넥터를 통해 상기 외부 컴퓨팅장치로부터 해당 시나리오에 대한 방어코드가 입력되어 방어시뮬레이션을 수행하고,

상기 방어코드는 상기 공격코드에 대응될 수 있도록 설계되는, 해커보드실습장치.

청구항 3

청구항 2에 있어서,

상기 제2MCU는 외부장치로부터 수신한 데이터 패킷에 기반하여 수행되는 동작에 대한 시스템동작코드가 상기 USB커넥터를 통해 코딩 되어 있고,

해당 동작은 상기 제2모듈장착부에 의해 물리적으로 구현이 되는, 해커보드실습장치.

청구항 4

청구항 3에 있어서,

상기 제1모듈장착부는 제1적외선송신센서 및 제1적외선수신센서를 더 포함하고,

상기 제2모듈장착부는 제2적외선송신센서 및 제2적외선수신센서를 더 포함하고,

상기 해커보드실습장치는 복수의 적외선공격시나리오 및 복수의 적외선방어시나리오를 포함하는 상기 적외선스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행하고,

상기 해커보드실습장치는,

상기 제1MCU에 의하여, 상기 외부장치로부터 상기 제2모듈장착부로 송신되는 데이터 패킷이 상기 제1적외선수신센서를 통해 스니핑되는 제1적외선공격시나리오;

상기 제1MCU에 의하여, 스니핑된 데이터 패킷이 상기 공격코드에 기반하여 위변조되는 제2적외선공격시나리오;

상기 제1MCU에 의하여, 상기 제1적외선송신센서를 통해 위변조된 데이터 패킷이 상기 제2모듈장착부로 송신되는 제3적외선공격시나리오;

상기 제2MCU에 의하여, 상기 제2적외선수신센서를 통해 상기 위변조된 데이터 패킷이 상기 제1적외선송신센서로부터 수신되는 제1적외선방어시나리오; 및

상기 제2MCU에 의하여, 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷에 의한 공격이 방어되는 제2적외선방어시나리오;를 수행하는, 해커보드실습장치.

청구항 5

청구항 3에 있어서,

상기 제1모듈장착부는 UART신호를 주고받는 제1UART모듈을 더 포함하고,

상기 제2모듈장착부는 UART신호를 주고받는 제2UART모듈을 더 포함하고,

상기 해커보드는,

상기 제1모듈장착부 및 제2모듈장착부를 연결하여 UART신호를 주고받는 UART커넥터; 및

상기 UART커넥터의 On/Off동작을 제어하는 UART스위치모듈;을 더 포함하고,

상기 해커보드실습장치는 복수의 UART공격시나리오 및 복수의 UART방어시나리오를 포함하는 상기 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행할 수 있고,

상기 해커보드실습장치는,

상기 제1MCU에 의하여, 상기 제1UART모듈을 통해 상기 외부장치로부터 상기 제2모듈장착부로 송신되는 데이터 패킷이 스니핑되는 제1UART공격시나리오;

상기 제1MCU에 의하여, 스니핑된 데이터 패킷이 상기 공격코드에 기반하여 위변조되는 제2UART공격시나리오;

상기 제1MCU에 의하여, 위변조된 데이터 패킷이 상기 제2모듈장착부로 송신되는 제3UART공격시나리오;

상기 제2MCU에 의하여, 상기 UART커넥터를 통해 상기 위변조된 데이터 패킷이 상기 제2모듈장착부로 수신되는 제1UART방어시나리오; 및

상기 제2MCU에 의하여, 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷에 의한 공격이 방어되는 제2UART방어시나리오;를 수행하는, 해커보드실습장치.

발명의 설명

기술 분야

[0001] 본 발명은 두 개의 MCU를 포함하는 해커보드실습장치로서, 하나의 케이스에 구비될 수 있는 해커보드에 포함된

제1MCU 및 제1MCU의 성능을 확장시키는 제1모듈장착부와 제2MCU 및 제2MCU의 성능을 확장시키는 제2모듈장착부를 통해 해킹교육에 있어 실습자가 하나의 해커보드실습장치를 이용하여 적외선신호 혹은 UART신호에 대한 모의해킹의 공격시뮬레이션 및 방어시뮬레이션을 동시에 수행할 수 있는, 두 개의 MCU를 포함하는 해커보드실습장치에 관한 것이다.

배경 기술

- [0003] 현대사회에서 정보기술은 눈에 띄게 빠른 속도로 발전하고, 다양한 산업을 이끌 수 있는 혁신적인 기술로 여겨지고 있으며, 현대인들의 일상생활에 필수적인 요소로 다가오고 있다. 이에 동시에 사물인터넷(Internet of Things)과 같이 사용자와 밀접하게 이루어지는 정보기술에 대한 보안위협은 기존의 보안위협과 달리 사용자의 신체, 재산에 대한 심각한 피해를 발생시킬 가능성이 있다.
- [0004] 최근 들어, 정보기술에 대한 해킹공격의 발생 빈도가 빈번해지고 있으며, 그 방법이 정교해지고 있다. 특히, UART는 범용 비동기화 송수신기(Universal Asynchronous Receiver/Transmitter)의 약자로, 사물인터넷 장비의 진단 및 디버깅 관련 보고에 사용되는 요소였으나, 누구나 쉽게 접근할 수 있다는 특징때문에, 해킹 공격자가 이를 통해 손쉽게 펌웨어를 다운로드 받고 취약점을 파악할 수 있다는 문제점이 발생하고 있다. 그러므로, 보안 업계는 해킹공격에 대해 끊임없이 감시하고 위험성을 알리며 이에 대한 해결책을 강구할 필요가 있다.
- [0005] 해킹공격을 방어하고 대응하기 위한 보안전문가를 양성하는 것이 전술한 해결책 중 하나가 될 수 있으며, 이를 위해서는 소프트웨어 기반의 지식교육과 함께 하드웨어 기반의 실습교육이 수반될 필요가 있다. 구체적으로 모의해킹은 이러한 교육의 일환으로서, 데이터 패킷이 포함된 신호를 송수신하는 모듈을 구성하고, 모의해킹을 수행하며 소스코드를 짜는 방식으로 이루어질 수 있다.
- [0006] 한편, 종래의 모듈을 이용한 해킹교육시스템으로는, 공격자모듈 및 방어자모듈이 따로 구비되어, 모의해킹에 대한 정확한 테스트 혹은 결과가 도출되지 못하였다. 또한, 실제 전자제품을 이용하여 모의해킹을 시도하기에는 현실적으로 무리가 있으므로, 공격자 및 방어자 역할을 수행할 수 있는 하나의 장치가 요구되는 상황이다.
- [0007] 그러므로 적외선신호 모의해킹 혹은 UART신호 모의해킹을 실습할 수 있는 장치를 제공하고, 하나의 장치를 통해 공격자 및 방어자를 동시에 수행하여 모의해킹에 대한 교육효율을 증대하는 기술의 개발이 필요한 상황이다.

발명의 내용

해결하려는 과제

- [0009] 본 발명은 두 개의 MCU를 포함하는 해커보드실습장치로서, 하나의 케이스에 구비될 수 있는 해커보드에 포함된 제1MCU 및 제1MCU의 성능을 확장시키는 제1모듈장착부와 제2MCU 및 제2MCU의 성능을 확장시키는 제2모듈장착부를 통해 해킹교육에 있어 실습자가 하나의 해커보드실습장치를 이용하여 적외선신호 혹은 UART신호에 대한 모의해킹의 공격시뮬레이션 및 방어시뮬레이션을 동시에 수행할 수 있는, 두 개의 MCU를 포함하는 해커보드실습장치를 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0011] 상기와 같은 과제를 해결하기 위하여 본 발명의 일 실시예에서는, 모의해킹에 대한 시뮬레이션을 수행하는 해커보드실습장치로서, 해커보드; 및 케이스;를 포함하고, 상기 해커보드는, 1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 모의해킹에 대한 공격시뮬레이션을 수행하는 제1MCU; 1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 모의해킹에 대한 방어시뮬레이션을 수행하는 제2MCU; 상기 제1MCU와 연결되고, 상기 공격시뮬레이션의 수행여부를 출력하는 부저 혹은 LED를 포함하는 복수의 전자모듈을 포함할 수 있는 제1모듈장착부; 상기 제2MCU와 연결되고, 상기 방어시뮬레이션의 수행여부를 출력하는 부저 혹은 LED를 포함하는 복수의 전자모듈을 포함할 수 있는 제2모듈장착부; 상기 제1MCU 및 상기 제2MCU를 외부 컴퓨팅장치와 연결하고, 상기 외부 컴퓨팅장치로부터 공격코드 및 방어코드를 수신하는 USB커넥터; 및 상기 제1MCU 및 상기 제2MCU에 대한 상기 USB커넥터의 연결을 제어하는 USB스위치모듈;을 포함하고, 상기 해커보드는 하나의 상기 케이스 내부에 설치될 수 있는, 해커보

드실습장치를 제공한다.

- [0012] 본 발명의 일 실시예에서는, 상기 해커보드실습장치는 적외선스니핑시나리오 혹은 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행하고, 상기 제1MCU는 공격자MCU로써, 상기 USB커넥터를 통해 상기 외부 컴퓨팅장치로부터 해당 시나리오에 대한 공격코드가 입력되어 공격시뮬레이션을 수행하고, 상기 제2MCU는 방어자MCU로써, 상기 USB커넥터를 통해 상기 외부 컴퓨팅장치로부터 해당 시나리오에 대한 방어코드가 입력되어 방어시뮬레이션을 수행하고, 상기 방어코드는 상기 공격코드에 대응될 수 있도록 설계될 수 있다.
- [0013] 본 발명의 일 실시예에서는, 상기 제2MCU는, 외부장치로부터 수신한 데이터 패킷에 기반하여 수행되는 동작에 대한 시스템동작코드가 상기 USB커넥터를 통해 코딩 되어 있고, 해당 동작은 상기 제2모듈장착부에 의해 물리적으로 구현이 될 수 있다.
- [0014] 본 발명의 일 실시예에서는, 상기 제1모듈장착부는 제1적외선송신센서 및 제1적외선수신센서를 더 포함하고, 상기 제2모듈장착부는 제2적외선송신센서 및 제2적외선수신센서를 더 포함하고, 상기 해커보드실습장치는 복수의 적외선공격시나리오 및 복수의 적외선방어시나리오를 포함하는 상기 적외선스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행하고, 상기 해커보드실습장치는, 상기 제1MCU에 의하여, 상기 외부장치로부터 상기 제2모듈장착부로 송신되는 데이터 패킷이 상기 제1적외선수신센서를 통해 스니핑되는 제1적외선공격시나리오; 상기 제1MCU에 의하여, 스니핑된 데이터 패킷이 상기 공격코드에 기반하여 위변조되는 제2적외선공격시나리오; 상기 제1MCU에 의하여, 상기 제1적외선송신센서를 통해 위변조된 데이터 패킷이 상기 제2모듈장착부로 송신되는 제3적외선공격시나리오; 상기 제2MCU에 의하여, 상기 제2적외선수신센서를 통해 상기 위변조된 데이터 패킷이 상기 제1적외선수신센서로부터 수신되는 제1적외선방어시나리오; 및 상기 제2MCU에 의하여, 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷에 의한 공격이 방어되는 제2적외선방어시나리오;를 수행할 수 있다.
- [0015] 본 발명의 일 실시예에서는, 상기 해커보드는, 상기 제1모듈장착부는 UART신호를 주고받는 제1UART모듈을 더 포함하고, 상기 제2모듈장착부는 UART신호를 주고받는 제2UART모듈을 더 포함하고, 상기 해커보드는, 상기 제1모듈장착부 및 제2모듈장착부를 연결하여 UART신호를 주고받는 UART커넥터; 및 상기 UART커넥터의 On/Off동작을 제어하는 UART스위치모듈;을 더 포함하고, 상기 해커보드실습장치는 복수의 UART공격시나리오 및 복수의 UART방어시나리오를 포함하는 상기 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행할 수 있고, 상기 해커보드실습장치는, 상기 제1MCU에 의하여, 상기 제1UART모듈을 통해 상기 외부장치로부터 상기 제2모듈장착부로 송신되는 데이터 패킷이 스니핑되는 제1UART공격시나리오; 상기 제1MCU에 의하여, 스니핑된 데이터 패킷이 상기 공격코드에 기반하여 위변조되는 제2UART공격시나리오; 상기 제1MCU에 의하여, 위변조된 데이터 패킷이 상기 제2모듈장착부로 송신되는 제3UART공격시나리오; 상기 제2MCU에 의하여, 상기 UART커넥터를 통해 상기 위변조된 데이터 패킷이 상기 제2모듈장착부로 수신되는 제1UART방어시나리오; 및 상기 제2MCU에 의하여, 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷에 의한 공격이 방어되는 제2UART방어시나리오;를 수행할 수 있다.

발명의 효과

- [0017] 본 발명의 일 실시예에서는, 두 개의 MCU를 포함하는 하나의 해커보드를 통해 모의해킹에 대한 공격시뮬레이션과 방어시뮬레이션이 동시에 수행됨으로써, 모의해킹 결과에 대한 즉각적인 피드백이 가능해져, 실습자에 대해 해당 모의해킹에 대한 교육효과가 강화되는 효과를 발휘할 수 있다.
- [0018] 본 발명의 일 실시예에서는, 상기 해커보드실습장치를 통해 실습하는 실습자들이 적외선신호에 대한 모의해킹을 실습함으로써, 적외선신호 해킹에 대한 교육효과를 강화하는 효과를 발휘할 수 있다.
- [0019] 본 발명의 일 실시예에서는, 상기 해커보드실습장치를 통해 실습하는 실습자들이 UART신호에 대한 모의해킹을 실습함으로써, UART신호 해킹에 대한 교육효과를 강화하는 효과를 발휘할 수 있다.
- [0020] 본 발명의 일 실시예에서는, 교육목적에 따라 제1모듈장착부 및 제2모듈장착부에 다양한 모듈을 포함시킴으로써, 다양한 종류의 모의해킹 실습이 가능해져 상기 해커보드실습장치를 이용하는 실습자들의 해당 모의해킹에 대한 교육효과가 강화되는 효과를 발휘할 수 있다.
- [0021] 본 발명의 일 실시예에서는, 상기 해커보드실습장치를 통해 실습하는 실습자들이 외부 컴퓨팅장치를 통해 시나리오에 따라 공격코드 및 방어코드를 작성하여 공격시뮬레이션 및 방어시뮬레이션을 수행함으로써, 모의해킹에 대한 교육효과를 강화하는 효과를 발휘할 수 있다.

도면의 간단한 설명

[0023]

도 1은 본 발명의 일 실시예에 따른 해커보드실습장치를 개략적으로 도시한다.

도 2는 본 발명의 일 실시예에 따른 외부 컴퓨팅장치를 통해 USB커넥터로 복수의 코드가 입력되는 과정을 개략적으로 도시한다.

도 3은 본 발명의 일 실시예에 따른 공격시뮬레이션 및 방어시뮬레이션의 수행과정을 개략적으로 도시한다.

도 4는 본 발명의 일 실시예에 따른 시스템동작코드가 코딩된 제2MCU의 동작을 개략적으로 도시한다.

도 5는 본 발명의 일 실시예에 따른 해커보드실습장치의 모의해킹에 대한 수행단계를 개략적으로 도시한다.

도 6은 본 발명의 일 실시예에 따른 적외선스니핑시나리오를 개략적으로 도시한다.

도 7은 본 발명의 일 실시예에 따른 UART스니핑시나리오를 개략적으로 도시한다.

도 8은 본 발명의 일 실시예에 따른 컴퓨팅장치의 내부 구성을 예시적으로 도시한다.

발명을 실시하기 위한 구체적인 내용

[0024]

이하에서는, 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 발명의 기술 분야에서 통상의 지식을 가진 자에게 인식될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다.

[0026]

또한, 다양한 양상들 및 특징들이 다수의 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있는 시스템에 의하여 제시될 것이다. 다양한 시스템들이, 추가적인 장치들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있다는 점 그리고/또는 도면들과 관련하여 논의된 장치들, 컴포넌트들, 모듈들 등 전부를 포함하지 않을 수도 있다는 점 또한 이해되고 인식되어야 한다.

[0027]

본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다. 아래에서 사용되는 용어들 '~부', '컴포넌트', '모듈', '시스템', '인터페이스' 등은 일반적으로 컴퓨터 관련 엔티티(computer-related entity)를 의미하며, 예를 들어, 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어를 의미할 수 있다.

[0028]

또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다.

[0029]

또한, 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0030]

또한, 본 발명의 실시예들에서, 별도로 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 발명의 실시예에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

- [0032] 도 1은 본 발명의 일 실시예에 따른 해커보드실습장치를 개략적으로 도시한다.
- [0034] 도 1에 도시된 바와 같이, 모의해킹에 대한 시뮬레이션을 수행하는 해커보드실습장치로서, 해커보드(1000); 및 케이스(2000);를 포함하고, 상기 해커보드(1000)는, 1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 모의해킹에 대한 공격시뮬레이션을 수행하는 제1MCU(1100); 1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 모의해킹에 대한 방어시뮬레이션을 수행하는 제2MCU(1200); 상기 제1MCU(1100)와 연결되고, 상기 공격시뮬레이션의 수행여부를 출력하는 부저 혹은 LED를 포함하는 복수의 전자모듈을 포함할 수 있는 제1모듈장착부(1300); 상기 제2MCU(1200)와 연결되고, 상기 방어시뮬레이션의 수행여부를 출력하는 부저 혹은 LED를 포함하는 복수의 전자모듈을 포함할 수 있는 제2모듈장착부(1400); 상기 제1MCU(1100) 및 상기 제2MCU(1200)를 외부 컴퓨팅장치와 연결하고, 상기 외부 컴퓨팅장치로부터 공격코드 및 방어코드를 수신하는 USB커넥터(1500); 및 상기 제1MCU(1100) 및 상기 제2MCU(1200)에 대한 상기 USB커넥터(1500)의 연결을 제어하는 USB스위치모듈(1600);을 포함하고, 상기 해커보드(1000)는 하나의 상기 케이스(2000) 내부에 설치될 수 있다.
- [0036] 개략적으로, 도 1의 (a)는 해커보드실습장치의 구조를 도시하고, 도 1의 (b)는 해커보드(1000)의 구조를 도시한다.
- [0038] 구체적으로, 도 1의 (a)에 도시된 바와 같이, 해커보드실습장치는 해커보드(1000) 및 케이스(2000)를 포함하며, 상기 해커보드(1000)는 하나의 상기 케이스(2000) 내부에 설치될 수 있어, 학교, 학원, 대학 등의 교육기관에서 모의해킹에 대한 교육을 받는 실습자들에게 높은 접근성을 제공하는 효과를 발휘할 수 있다.
- [0039] 또한, 도 1의 (b)에 도시된 바와 같이, 상기 해커보드(1000)는 제1MCU(1100), 제2MCU(1200), 제1모듈장착부(1300), 제2모듈장착부(1400), USB커넥터(1500) 및 USB스위치모듈(1600)을 포함할 수 있으며, 본 발명의 다른 실시예에서 해커보드(1000)는, 도 1의 (b)에 도시된 부품에 한정하지 아니하고, 모의해킹에 대한 교육의 목적에 따라 다양한 종류의 부품을 포함할 수 있다.
- [0040] 상기 제1MCU(1100)는 1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 실습자의 조작에 따라 모의해킹에 대한 공격시뮬레이션을 수행한다. 바람직하게, 상기 해커보드실습장치가 수행하는 공격시뮬레이션은 실습자가 실습하고자 하는 모의해킹에 대한 공격시나리오에 따라 상이해질 수 있다.
- [0041] 상기 제2MCU(1200)는 1 이상의 프로세서 및 1 이상의 메모리를 포함하고, 실습자의 조작에 따라 모의해킹에 대한 방어시뮬레이션을 수행한다. 바람직하게, 상기 해커보드실습장치가 수행하는 방어시뮬레이션은 실습자가 실습하고자 하는 모의해킹에 대한 방어시나리오에 따라 상이해질 수 있다.
- [0042] 상기 제1모듈장착부(1300)는 상기 해커보드(1000)를 통해 상기 제1MCU(1100)와 연결되고, 상기 제2모듈장착부(1400)는 상기 해커보드(1000)를 통해 상기 제2MCU(1200)와 연결되며, 상기 제1모듈장착부(1300) 및 제2모듈장착부(1400)는 실습자의 교육목적에 따라 다양한 전자모듈을 장착 형태로서 포함할 수 있다. 바람직하게, 상기 제1모듈장착부(1300)는 공격시뮬레이션을 수행하기 위한 전자모듈을 포함하고, 상기 제2모듈장착부(1400)는 방어시뮬레이션을 수행하기 위한 전자모듈을 포함한다. 예를 들어, 상기 제1모듈장착부(1300) 및 상기 제2모듈장착부(1400) 각각은 적외선센서, RF센서 등의 전자모듈을 더 포함시켜, 상기 해커보드실습장치가 해당 전자모듈 각각을 통해 모의해킹에 대한 다양한 시뮬레이션을 수행할 수 있도록 함으로써, 실습자에 대한 교육효과를 높이는 효과를 발휘할 수 있다.
- [0043] 또한, 부저 혹은 LED는 상기 제1모듈장착부(1300) 및 제2모듈장착부(1400) 각각에 포함될 수 있다. 상기 제1MCU(1100)에서 공격시뮬레이션이 정상적으로 수행된 경우, 상기 제1모듈장착부(1300)에 포함된 부저 혹은 LED가 작동되어 실습자에게 공격시뮬레이션의 정상적인 작동을 인지시키고, 상기 제2MCU(1200)에서 방어시뮬레이션이 정상적으로 수행된 경우, 상기 제2모듈장착부(1400)에 포함된 부저 혹은 LED가 작동되어 실습자에게 방어시뮬레이션의 정상적인 작동을 인지시킨다.
- [0044] 상기 USB커넥터(1500)는 USB선을 통해 상기 제1MCU(1100) 및 상기 제2MCU(1200)를 외부 컴퓨팅장치와 연결하고, 상기 외부 컴퓨팅장치로부터 공격코드 및 방어코드를 수신한다. 본 발명의 일 실시예에서, 상기 USB커넥터(1500)는 해커보드(1000)와 외부 컴퓨팅장치를 연결하는 상기 USB선의 형태에 따라 A-Type포트, B-Type포트 혹은 C-Type포트일 수 있으며, 본 발명의 다른 실시예에서, 상기 해커보드(1000)는 서로 다른 타입의 포트인 복수

의 USB커넥터(1500)를 더 포함하여 실습자에게 상기 해커보드실습장치 이용에 대한 편리함을 제공하는 효과를 발휘할 수 있다.

[0045] 상기 USB스위치모듈(1600)은 상기 제1MCU(1100) 및 상기 제2MCU(1200) 각각에 대한 상기 USB커넥터(1500)의 연결을 제어한다. 도 1의 (b)에 도시된 ATT스위치는 공격자(Attacker)역할을 수행하는 제1MCU(1100)와 상기 외부 컴퓨팅장치의 연결을 제어하고, DEF스위치는 방어자(Defender)역할을 수행하는 제2MCU(1200)와 상기 외부 컴퓨팅장치의 연결을 제어한다.

[0046] 더 구체적으로, 스위치가 USB쪽으로 조작된 경우, 해당 스위치에 대한 MCU만 상기 외부 컴퓨팅장치와 연결되고, 상기 ATT스위치 및 DEF스위치가 HUB쪽으로 조작된 경우, 상기 제1MCU(1100) 및 제2MCU(1200)가 동시에 상기 외부 컴퓨팅장치와 연결됨으로써, 실습자에게 상기 해커보드실습장치 이용에 대한 편리함을 제공하는 효과를 발휘할 수 있다.

[0047] 또한, 바람직하게 상기 해커보드(1000)는 외부전원과 연결될 수 있도록 상기 해커보드(1000)에 전원을 공급하는 외부전원소켓 등을 더 포함할 수 있다.

[0049] 도 2는 본 발명의 일 실시예에 따른 외부 컴퓨팅장치를 통해 USB커넥터(1500)로 복수의 코드가 입력되는 과정을 개략적으로 도시한다.

[0051] 도 2에 도시된 바와 같이, 상기 모의해킹에 대한 시뮬레이션은 적외선스니핑시나리오 및 UART스니핑시나리오를 포함하고, 상기 제1MCU(1100)는 공격자MCU로써, 상기 USB커넥터(1500)를 통해 상기 외부 컴퓨팅장치로부터 해당 시나리오에 대한 공격코드가 입력되어 공격시뮬레이션을 수행하고, 상기 제2MCU(1200)는 방어자MCU로써, 상기 USB커넥터(1500)를 통해 상기 외부 컴퓨팅장치로부터 해당 시나리오에 대한 방어코드가 입력되어 방어시뮬레이션을 수행하고, 상기 방어코드는 상기 공격코드에 대응될 수 있도록 설계된다.

[0053] 구체적으로, 상기 해커보드(1000)는 상기 USB커넥터(1500)를 통해 상기 외부 컴퓨팅장치로부터 공격코드 및 방어코드를 수신한다. 더 구체적으로, 상기 공격코드 및 방어코드는 실습자에 의해 모의해킹에 대한 시뮬레이션마다 다르게 설계될 수 있고, 바람직하게, 도 3에 도시된 바와 같이, 공격시뮬레이션을 수행하는 제1MCU(1100)에 공격코드가 입력되고, 방어시뮬레이션을 수행하는 제2MCU(1200)에 방어코드가 입력되며, 이 때, 상기 방어코드는 상기 공격코드의 공격 형태에 대응될 수 있도록 설계된다.

[0054] 실습자는 상기 해커보드실습장치를 통해 모의해킹에 대한 공격시뮬레이션 및 방어시뮬레이션을 동시에 수행하고, 즉각적으로 도출되는 해당 시뮬레이션의 결과에서 발견되는 문제점 혹은 오류를 통해 해당 시뮬레이션에서 사용된 공격코드 혹은 방어코드에 대한 교육을 함으로써, 상기 해커보드실습장치가 모의해킹에 대해 실습자에게 높은 교육효과를 제공하는 효과를 발휘할 수 있다.

[0055] 또한 상기 해커보드실습장치는 적외선스니핑시나리오 혹은 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행하고, 상기 적외선스니핑시나리오 및 UART스니핑시나리오 각각은 해당 시나리오에 대한 공격시나리오 및 방어시나리오를 포함한다. 바람직하게, 상기 공격코드는 공격시나리오에 상응하도록, 상기 방어코드는 상기 방어시나리오에 상응하도록 설계된다. 예를 들어, 실습자가 모의해킹에 대한 공격시뮬레이션이 적외선스니핑시나리오에 포함된 적외선공격시나리오에 기반하여 수행되기를 원하는 경우, 상기 실습자는 상기 적외선공격시나리오에 대한 공격시뮬레이션을 수행하기 위한 공격코드를 상기 외부 컴퓨팅장치에 입력하는 것이 바람직하다.

[0057] 한편, 본 발명의 다른 실시예에서, 상기 해커보드실습장치는 데이터 스푸핑(Spoofing), 스누핑(Snooping) 등과 같은 다양한 공격유형에 따른 모의해킹에 대한 복수의 시뮬레이션을 더 수행할 수 있다.

[0059] 도 4는 본 발명의 일 실시예에 따른 시스템동작코드가 코딩된 제2MCU(1200)의 동작을 개략적으로 도시한다.

- [0061] 도 4에 도시된 바와 같이, 상기 제2MCU(1200)는, 외부장치로부터 수신한 데이터 패킷에 기반하여 수행되는 동작에 대한 시스템동작코드가 상기 USB커넥터(1500)를 통해 코딩되어 있고, 해당 동작은 상기 제2모듈장착부(1400)에 의해 물리적으로 구현이 된다.
- [0063] 일반적으로, 현대사회에서의 전자기기들의 상호 조작 간에는 데이터 패킷을 포함한 신호가 주고받아지고, 주로 해커는 이러한 신호를 이용하여 해킹공격을 한다. 예를 들어, TV의 음량조절을 위해서는 리모컨으로부터 TV로 송신되는 신호가 필요하며, 해커는 해당 신호에 포함된 음량조절 명령정보를 위변조하고, TV의 음량조절에 대한 동작을 다른 동작으로 변형시켜 해당 TV를 보는 사용자를 공격할 수 있다.
- [0064] 바람직하게, 실제 전자기기에서 송수신되는 신호를 해킹하여 상기 실제 전자기기를 조작하는 방법으로 해킹보안에 대한 교육을 수행하기에는 현실적으로 비용적인 문제가 발생할 수 있고, 큰 위험이 감수되어야 하므로, 본 발명에서의 상기 해커보드실습장치는 전술한 상황과 같이, 신호에 포함된 데이터 패킷의 모의해킹에 대한 시뮬레이션을 수행한다. 본 발명의 일 실시예로서, 데이터 패킷을 포함한 신호를 해킹하여 위변조된 신호를 송신하는 전자기기의 역할을 제1MCU(1100)가 수행하고, 위변조된 신호를 수신하는 전자기기의 역할을 제2MCU(1200)가 수행한다.
- [0066] 구체적으로, 리모컨에 의해 TV의 음량이 조절되는 것과 같이, 외부장치로부터 송신되는 데이터 패킷에 기반하여 전자기기가 특정 동작을 수행한다고 할 때, 실습자는 상기 외부 컴퓨팅장치에 상기 해커보드(1000)가 해당 동작을 수행할 수 있도록 하는 시스템동작코드를 입력할 필요가 있다.
- [0067] 이후, 상기 외부 컴퓨팅장치에 입력된 시스템동작코드가 상기 USB커넥터(1500)를 통해 상기 제2MCU(1200)에 코딩됨으로써, 상기 데이터 패킷에 기반하여 수행되는 동작은 해당 시스템동작코드에 따라 상기 제2모듈장착부(1400)에 의해 물리적으로 구현될 수 있으며, 부저 혹은 LED의 동작을 통해 해당 동작이 구현됨이 간접적으로 표시될 수 있다. 한편 본 발명의 다른 실시예에서는, 상기 시스템동작코드는 상기 외부 컴퓨팅장치에 기저장된 코드일 수 있다. 이후, 전술한 데이터 패킷을 포함한 신호를 이용하여 수행되는 모의해킹에 대한 시뮬레이션의 자세한 설명은 도 5에서 후술하도록 한다.
- [0069] 도 5는 본 발명의 일 실시예에 따른 해커보드실습장치의 모의해킹에 대한 수행단계를 개략적으로 도시한다.
- [0071] 해커보드실습장치가 모의해킹에 대한 시뮬레이션을 수행하기 위해서는, 우선 해커보드실습장치를 이용하는 실습자가 교육을 원하는 시뮬레이션을 선택(S10)할 필요가 있다. 해당 시뮬레이션은 본 발명의 일 실시예로서, 도 4에 도시된 바와 같이, TV-리모컨간에 송수신되는 데이터 패킷을 해킹하는 시나리오에 해당할 수 있다.
- [0072] 실습자의 시뮬레이션 선택 이후, 상기 실습자는 자신이 선택한 해당 시뮬레이션에 대한 공격코드, 방어코드 및 시스템동작코드를 상기 외부 컴퓨팅장치에 입력(S20)한다.
- [0073] 상기 제1모듈장착부(1300)는 실습자에 의해, 해당 시뮬레이션에 대해 요구되는 전자모듈을 포함하도록 설계되고, 상기 제2모듈장착부(1400) 또한 실습자에 의해, 해당 시뮬레이션에 대해 요구되는 전자모듈을 포함하도록 설계(S30)된다.
- [0074] 이후, 제1MCU(1100)는 외부장치로부터 제2모듈장착부(1400)로 송신되는 데이터 패킷을 제1모듈장착부(1300)를 통해 스니핑(S40)하고, 상기 외부 컴퓨팅장치로부터 입력 받은(S20) 공격코드에 기반하여 스니핑한 데이터 패킷을 위변조(S50)하고, 위변조된 데이터 패킷을 상기 제2모듈장착부(1400)로 송신함(S60)으로써, 모의해킹에 대한 공격시뮬레이션을 수행한다.
- [0075] 제2MCU(1200)는 위변조된 데이터 패킷을 상기 제2모듈장착부(1400)를 통해 수신(S70)하고, 상기 외부 컴퓨팅장치로부터 입력 받은(S20) 방어코드에 기반하여 상기 위변조된 데이터 패킷의 공격을 감지하고, 이에 대한 방어(S80)를 함으로써, 모의해킹에 대한 방어시뮬레이션을 수행한다.
- [0077] 이와 같이 해커보드실습장치는 하나의 장치로서 모의해킹에 대한 공격시뮬레이션 및 방어시뮬레이션을 동시에

수행하고, 도출되는 시뮬레이션 결과에 따라 실습자가 공격코드 및 방어코드에 대한 즉각적인 피드백이 가능하게 하여, 해당 해커보드실습장치를 이용하는 실습자에게 높은 교육효과를 제공하는 효과를 발휘할 수 있다.

[0079] 도 6은 본 발명의 일 실시예에 따른 적외선스니핑시나리오를 개략적으로 도시한다.

[0081] 도 6에 도시된 바와 같이, 상기 제1모듈장착부(1300)는 제1적외선송신센서(1310) 및 제1적외선수신센서(1320)를 더 포함하고, 상기 제2모듈장착부(1400)는 제2적외선송신센서(1410) 및 제2적외선수신센서(1420)를 더 포함하고, 상기 해커보드실습장치는 복수의 적외선공격시나리오 및 복수의 적외선방어시나리오를 포함하는 상기 적외선스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행하고, 상기 해커보드실습장치는, 상기 제1MCU(1100)에 의하여, 상기 외부장치로부터 상기 제2모듈장착부(1400)로 송신되는 데이터 패킷이 상기 제1적외선수신센서(1320)를 통해 스니핑되는 제1적외선공격시나리오; 상기 제1MCU(1100)에 의하여, 스니핑된 데이터 패킷이 상기 공격코드에 기반하여 위변조되는 제2적외선공격시나리오; 상기 제1MCU(1100)에 의하여, 상기 제1적외선송신센서(1310)를 통해 위변조된 데이터 패킷이 상기 제2모듈장착부(1400)로 송신되는 제3적외선공격시나리오; 상기 제2MCU(1200)에 의하여, 상기 제2적외선수신센서(1420)를 통해 상기 위변조된 데이터 패킷이 상기 제1적외선송신센서(1310)로부터 수신되는 제1적외선방어시나리오; 및 상기 제2MCU(1200)에 의하여, 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷에 의한 공격이 방어되는 제2적외선방어시나리오;를 수행한다.

[0083] 상기 해커보드실습장치는 실습자의 교육 목적에 따라 다양한 모듈을 제1모듈장착부(1300) 및 제2모듈장착부(1400) 각각에 포함시킬 수 있다. 도 6에 도시된 본 발명의 일 실시예에서, 상기 해커보드실습장치는 적외선스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행할 수 있으며, 이를 위해 상기 제1모듈장착부(1300)는 제1적외선송신센서(1310) 및 제1적외선수신센서(1320)를 더 포함하고, 상기 제2모듈장착부(1400)는 제2적외선송신센서(1410) 및 제2적외선수신센서(1420)를 더 포함한다.

[0084] 바람직하게, 상기 제1적외선송신센서(1310) 및 상기 제2적외선송신센서(1410)는 동일한 구조의 센서이고, 상기 제1적외선수신센서(1320) 및 상기 제2적외선수신센서(1420)는 동일한 구조의 센서일 수 있다.

[0085] 도 6에 도시된 바와 같이, 상기 적외선스니핑시나리오는 외부장치로부터 제2적외선수신센서(1420)로 송신되는 데이터 패킷이 제1적외선수신센서(1320)를 통해 스니핑(Sniffing)되고(①), 스니핑된 데이터 패킷이 상기 제1MCU(1100)에 의해 위변조되고(②), 위변조된 데이터 패킷이 상기 제2적외선수신센서(1420)로 송신됨(③)으로써, 기존 적외선신호에 의해 구현되어야 하는 물리적인 동작이 비정상적인 동작으로 변형되고, 이러한 공격에 대응하여 방어를 하는(④) 과정이다.

[0086] 구체적으로, 상기 적외선스니핑시나리오는 복수의 적외선공격시나리오 및 복수의 적외선방어시나리오를 포함하며, 제1적외선공격시나리오 내지 제3적외선공격시나리오는 상기 제1MCU(1100)에 의해 수행되고, 제1적외선방어시나리오 내지 제2적외선방어시나리오는 상기 제2MCU(1200)에 의해 수행된다.

[0087] 제1적외선공격시나리오는 상기 도 5에서 전술한 리모컨과 같이 신호를 송출하는 외부장치로부터 상기 제2모듈장착부(1400)로 데이터 패킷이 송신될 때, 상기 제1적외선수신센서(1320)가 해당 데이터 패킷을 포함하는 적외선신호를 스니핑하는 과정이다.

[0088] 제2적외선공격시나리오는 상기 제1적외선수신센서(1320)에 의해 스니핑된 데이터 패킷을 상기 제1MCU(1100)가 상기 외부 컴퓨팅장치로부터 수신했던 공격코드에 기반하여 위변조하는 과정이다.

[0089] 바람직하게 해당 공격코드는 기존 데이터 패킷에 포함되어 상기 제2모듈장착부(1400)에 의해 구현되어야 하는 동작을 다른 동작으로 변형할 수 있도록 설계되어, 해당 공격코드에 기반하여 위변조된 데이터 패킷은 모의해킹에 대한 시뮬레이션 중 공격수단으로서의 역할을 수행한다.

[0090] 제3적외선공격시나리오는 상기 제2적외선공격시나리오를 통해 위변조된 데이터 패킷이 상기 제1적외선송신센서(1310)를 통해 상기 제2적외선수신센서(1420)로 송신되는 과정이다.

[0091] 제1적외선방어시나리오는 상기 제3적외선공격시나리오에서 위변조된 데이터 패킷이 상기 제2적외선수신센서(1420)를 통해 수신되는 과정이다.

- [0092] 제2적외선방어시나리오는 상기 제1적외선방어시나리오를 통해 수신한 상기 위변조된 데이터 패킷을 상기 제2MCU(1200)가 상기 외부 컴퓨팅장치로부터 수신했던 방어코드에 기반하여 방어하는 과정이다. 더 구체적으로, 상기 제2MCU(1200)는 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷을 정상적인 데이터 패킷과 구별하여 상기 위변조된 데이터 패킷을 감지하고, 상기 위변조된 데이터 패킷에 따른 동작을 무효화함으로써, 해당 시스템의 안정성을 강화한다.
- [0094] 도 7은 본 발명의 일 실시예에 따른 UART스니핑시나리오를 개략적으로 도시한다.
- [0096] 도 7에 도시된 바와 같이, 상기 제1모듈장착부(1300)는 UART신호를 주고받는 제1UART모듈(1330)을 더 포함하고, 상기 제2모듈장착부(1400)는 UART신호를 주고받는 제2UART모듈(1430)을 더 포함하고, 상기 해커보드(1000)는, 상기 제1모듈장착부(1300) 및 제2모듈장착부(1400)를 연결하여 UART신호를 주고받는 UART커넥터(1700); 및 상기 UART커넥터(1700)의 On/Off동작을 제어하는 UART스위치모듈(1800);을 더 포함하고, 상기 해커보드실습장치는 복수의 UART공격시나리오 및 복수의 UART방어시나리오를 포함하는 상기 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행할 수 있고, 상기 해커보드실습장치는, 상기 제1MCU(1100)에 의하여, 상기 제1UART모듈(1330)을 통해 상기 외부장치로부터 상기 제2모듈장착부(1400)로 송신되는 데이터 패킷이 스니핑되는 제1UART공격시나리오; 상기 제1MCU(1100)에 의하여, 스니핑된 데이터 패킷이 상기 공격코드에 기반하여 위변조되는 제2UART공격시나리오; 상기 제1MCU(1100)에 의하여, 위변조된 데이터 패킷이 상기 제2모듈장착부(1400)로 송신되는 제3UART공격시나리오; 상기 제2MCU(1200)에 의하여, 상기 UART커넥터(1700)를 통해 상기 위변조된 데이터 패킷이 상기 제2모듈장착부(1400)로 수신되는 제1UART방어시나리오; 및 상기 제2MCU(1200)에 의하여, 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷에 의한 공격이 방어되는 제2UART방어시나리오;를 수행한다.
- [0098] 도 6에서 전술한 바와 같이, 상기 해커보드실습장치는 실습자의 교육 목적에 따라 다양한 모듈을 제1모듈장착부(1300) 및 제2모듈장착부(1400)에 포함시킬 수 있으며, 도 7에 도시된 본 발명의 일 실시예에서, 상기 해커보드실습장치는 UART스니핑시나리오에 해당하는 모의해킹에 대한 시뮬레이션을 수행할 수 있으며, 이를 위해 상기 제1모듈장착부(1300)는 UART신호를 주고받는 제1UART모듈(1330)을 더 포함하고, 상기 제2모듈장착부(1400)는 UART신호를 주고받는 제2UART모듈(1430)을 더 포함하고, 상기 해커보드(1000)가 상기 제1모듈장착부(1300) 및 제2모듈장착부(1400)를 연결하는 UART커넥터(1700)를 더 포함하여, 상기 UART커넥터(1700)를 통해 상기 제1UART모듈(1330)과 상기 제2UART모듈(1430) 간에 UART신호가 주고받아질 수 있도록 한다.
- [0099] 바람직하게, 상기 제1UART모듈(1330) 및 상기 제2UART모듈(1430)은 동일한 구조의 모듈일 수 있다.
- [0100] 도 7에 도시된 바와 같이, 상기 UART스니핑시나리오는 외부장치로부터 제2UART모듈(1430)로 송신되는 UART신호에 포함된 데이터 패킷이 제1UART모듈(1330)로부터 스니핑되고(①), 스니핑된 데이터 패킷이 상기 제1MCU(1100)에 의해 위변조되고(②), 위변조된 데이터 패킷이 상기 제2UART모듈(1430)로 송신됨(③)으로써, 기존 UART신호에 의해 구현되어야 하는 물리적인 동작이 비정상적인 동작으로 변형되고, 이러한 공격에 대응하여 방어를 하는(④) 과정이다.
- [0101] 구체적으로, 상기 UART스니핑시나리오는 복수의 UART공격시나리오 및 복수의 UART방어시나리오를 포함하며, 제1UART공격시나리오 내지 제3UART공격시나리오는 상기 제1MCU(1100)에 의해 수행되고, 제1UART방어시나리오 내지 제2UART방어시나리오는 상기 제2MCU(1200)에 의해 수행된다.
- [0102] 제1UART공격시나리오는 상기 도 5에서 전술한 리모컨과 같이 신호를 송출하는 외부장치로부터 상기 제2모듈장착부(1400)로 데이터 패킷이 송신될 때, 상기 제1UART모듈(1330)이 해당 데이터 패킷을 포함하는 UART신호를 스니핑하는 과정이다.
- [0103] 제2UART공격시나리오는 상기 제1UART모듈(1330)에 의해 스니핑된 데이터 패킷을 상기 제1MCU(1100)가 상기 외부 컴퓨팅장치로부터 수신했던 공격코드에 기반하여 위변조하는 과정이다.
- [0104] 제3UART공격시나리오는 상기 제2UART공격시나리오를 통해 위변조된 데이터 패킷이 상기 UART커넥터(1700)를 통해 상기 제2모듈장착부(1400)로 송신되는 과정이다. 즉, 상기 위변조된 데이터 패킷은 상기 제1UART모듈(1330)에서 UART커넥터(1700)를 지나 제2UART모듈(1430)로 이동한다.

- [0105] 이 때, 상기 해커보드(1000)는 상기 UART커넥터(1700)의 UART신호의 통신 수행에 대한 On/Off동작을 제어하는 UART스위치모듈(1800)을 더 포함하고, 도 7에 도시된 UART스위치모듈(1800)의 스위치가 CON쪽으로 조작되는 경우, UART커넥터(1700)를 통해 UART신호가 송수신되고, N.C쪽으로 조작되는 경우, UART커넥터(1700)를 통해 UART신호가 송수신되지 않는다. 이와 같이, 실습자는 본인이 원하는 설계에 따라 상기 UART스위치모듈(1800)을 조작함으로써, 해당 모의해킹에 대한 시뮬레이션이 교육목적에 따라 용이하게 수행되도록 하는 효과는 발휘할 수 있다.
- [0106] 제1UART방어시나리오는 상기 제3UART공격시나리오에서 위변조된 데이터 패킷이 상기 UART커넥터(1700)를 통해 수신되는 과정이다.
- [0107] 제2UART방어시나리오는 상기 제1UART방어시나리오를 통해 수신한 상기 위변조된 데이터 패킷을 상기 제2MCU(1200)가 상기 외부 컴퓨팅장치로부터 수신했던 방어코드에 기반하여 방어하는 과정이다. 더 구체적으로, 상기 제2MCU(1200)는 상기 방어코드에 기반하여 상기 위변조된 데이터 패킷을 정상적인 데이터 패킷과 구별하여 상기 위변조된 데이터 패킷을 감지하고, 상기 위변조된 데이터 패킷에 따른 동작을 무효화함으로써, 해당 시스템의 안정성을 강화한다.
- [0109] 한편, 일반적으로 공격코드는 실습자에 의해 정상적인 코드로 위장되거나 변형되어 설계되므로, 방어코드에 의해 바로 감지되기 어렵기 때문에, 상기 해커보드실습장치를 이용하는 실습자는 상기 제2적외선방어시나리오의 수행결과 혹은 상기 제2UART방어시나리오의 수행결과를 피드백하여 방어코드를 계속해서 수정할 필요가 있다.
- [0110] 이와 같이, 하나의 장치로 구성된 상기 해커보드실습장치를 통해 실습자는 모의해킹에 대해 공격시뮬레이션의 결과 및 해당 공격시뮬레이션에 따른 방어시뮬레이션의 결과를 동시에 관찰함에 따라 즉각적인 피드백을 수행할 수 있으므로 상기 해커보드실습장치는 실습자에게 모의해킹에 대한 높은 교육효과를 제공하는 효과를 발휘할 수 있다.
- [0112] 도 8은 본 발명의 일 실시예에 따른 컴퓨팅장치(11000)의 내부 구성을 예시적으로 도시한다.
- [0114] 도 1에 대한 설명에서 언급된 제1MCU(1100) 및 제2MCU(1200)는 후술하는 도 8에 도시된 컴퓨팅장치(11000)의 구성요소를 포함할 수 있다.
- [0116] 도 8에 도시한 바와 같이, 컴퓨팅장치(11000)은 적어도 하나의 프로세서(processor)(11100), 메모리(memory)(11200), 주변장치 인터페이스(peripheral interface)(11300), 입/출력 서브시스템(I/O subsystem)(11400), 전력 회로(11500) 및 통신 회로(11600)를 적어도 포함할 수 있다.
- [0118] 구체적으로, 상기 메모리(11200)는, 일례로 고속 랜덤 액세스 메모리(high-speed random access memory), 자기 디스크, 에스램(SRAM), 디램(DRAM), 롬(ROM), 플래시 메모리 또는 비휘발성 메모리를 포함할 수 있다. 상기 메모리(11200)는 상기 컴퓨팅장치(11000)의 동작에 필요한 소프트웨어 모듈, 명령어 집합 또는 그 밖에 다양한 데이터를 포함할 수 있다.
- [0119] 이때, 상기 프로세서(11100)나 상기 주변장치 인터페이스(11300) 등의 다른 컴포넌트에서 상기 메모리(11200)에 액세스하는 것은 상기 프로세서(11100)에 의해 제어될 수 있다. 상기 프로세서(11100)은 단일 혹은 복수로 구성될 수 있고, 연산처리속도 향상을 위하여 GPU 및 TPU 형태의 프로세서를 포함할 수 있다.
- [0120] 상기 주변장치 인터페이스(11300)는 상기 컴퓨팅장치(11000)의 입력 및/또는 출력 주변장치를 상기 프로세서(11100) 및 상기 메모리(11200)에 결합시킬 수 있다. 상기 프로세서(11100)는 상기 메모리(11200)에 저장된 소프트웨어 모듈 또는 명령어 집합을 실행하여 상기 컴퓨팅장치(11000)을 위한 다양한 기능을 수행하고 데이터를 처리할 수 있다.
- [0121] 상기 입/출력 서브시스템(11400)은 다양한 입/출력 주변장치들을 상기 주변장치 인터페이스(11300)에 결합시킬 수 있다. 예를 들어, 상기 입/출력 서브시스템(11400)은 모니터나 키보드, 마우스, 프린터 또는 필요에 따라 터

치스크린이나 센서 등의 주변장치를 상기 주변장치 인터페이스(11300)에 결합시키기 위한 컨트롤러를 포함할 수 있다. 다른 측면에 따르면, 상기 입/출력 주변장치들은 상기 입/출력 서브시스템(11400)을 거치지 않고 상기 주변장치 인터페이스(11300)에 결합될 수도 있다.

[0122] 상기 전력 회로(11500)는 단말기의 컴포넌트의 전부 또는 일부로 전력을 공급할 수 있다. 예를 들어 상기 전력 회로(11500)는 전력 관리 시스템, 배터리나 교류(AC) 등과 같은 하나 이상의 전원, 충전 시스템, 전력 실패 감지 회로(power failure detection circuit), 전력 변환기나 인버터, 전력 상태 표시자 또는 전력 생성, 관리, 분배를 위한 임의의 다른 컴포넌트들을 포함할 수 있다.

[0123] 상기 통신 회로(11600)는 적어도 하나의 외부 포트를 이용하여 다른 컴퓨팅장치와 통신을 가능하게 할 수 있다. 또는, 상술한 바와 같이 필요에 따라 상기 통신 회로(11600)는 RF 회로를 포함하여 전자기 신호(electromagnetic signal)라고도 알려진 RF 신호를 송수신함으로써, 다른 컴퓨팅장치와 통신을 가능하게 할 수도 있다.

[0125] 이러한 도 8의 실시예는, 상기 컴퓨팅장치(11000)의 일례일 뿐이고, 상기 컴퓨팅장치(11000)는 도 8에 도시된 일부 컴포넌트가 생략되거나, 도 8에 도시되지 않은 추가의 컴포넌트를 더 구비하거나, 2 개 이상의 컴포넌트를 결합시키는 구성 또는 배치를 가질 수 있다. 예를 들어, 모바일 환경의 통신 단말을 위한 컴퓨팅장치는 도 8에 도시된 컴포넌트들 외에도, 터치스크린이나 센서 등을 더 포함할 수도 있으며, 상기 통신 회로(11600)에 다양한 통신방식(Wi-Fi, 3G, LTE, 5G, 6G, Bluetooth, NFC, Zigbee 등)의 RF 통신을 위한 회로가 포함될 수도 있다. 상기 컴퓨팅장치(11000)에 포함 가능한 컴포넌트들은 하나 이상의 신호 처리 또는 어플리케이션에 특화된 집적 회로를 포함하는 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어 양자의 조합으로 구현될 수 있다.

[0126] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨팅장치를 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 특히, 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다. 본 발명이 적용되는 어플리케이션은 파일 배포 시스템이 제공하는 파일을 통해 사용자 단말에 설치될 수 있다. 일 예로, 파일 배포 시스템은 사용자 단말이기의 요청에 따라 상기 파일을 전송하는 파일 전송부(미도시)를 포함할 수 있다.

[0128] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0129] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨팅장치 상에 표준편차되어서, 표준편차된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0130] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을

단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

- [0132] 본 발명의 일 실시예에서는, 두 개의 MCU를 포함하는 하나의 해커보드를 통해 모의해킹에 대한 공격시뮬레이션과 방어시뮬레이션이 동시에 수행됨으로써, 모의해킹 결과에 대한 즉각적인 피드백이 가능해져, 실습자에 대해 해당 모의해킹에 대한 교육효과가 강화되는 효과를 발휘할 수 있다.
- [0133] 본 발명의 일 실시예에서는, 상기 해커보드실습장치를 통해 실습하는 실습자들이 적외선신호에 대한 모의해킹을 실습함으로써, 적외선신호 해킹에 대한 교육효과를 강화하는 효과를 발휘할 수 있다.
- [0134] 본 발명의 일 실시예에서는, 상기 해커보드실습장치를 통해 실습하는 실습자들이 UART신호에 대한 모의해킹을 실습함으로써, UART신호 해킹에 대한 교육효과를 강화하는 효과를 발휘할 수 있다.
- [0135] 본 발명의 일 실시예에서는, 교육목적에 따라 제1모듈장착부 및 제2모듈장착부에 다양한 모듈을 포함시킴으로써, 다양한 종류의 모의해킹 실습이 가능해져 상기 해커보드실습장치를 이용하는 실습자들의 해당 모의해킹에 대한 교육효과가 강화되는 효과를 발휘할 수 있다.
- [0136] 본 발명의 일 실시예에서는, 상기 해커보드실습장치를 통해 실습하는 실습자들이 외부 컴퓨팅장치를 통해 시나리오에 따라 공격코드 및 방어코드를 작성하여 공격시뮬레이션 및 방어시뮬레이션을 수행함으로써, 모의해킹에 대한 교육효과를 강화하는 효과를 발휘할 수 있다.
- [0138] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

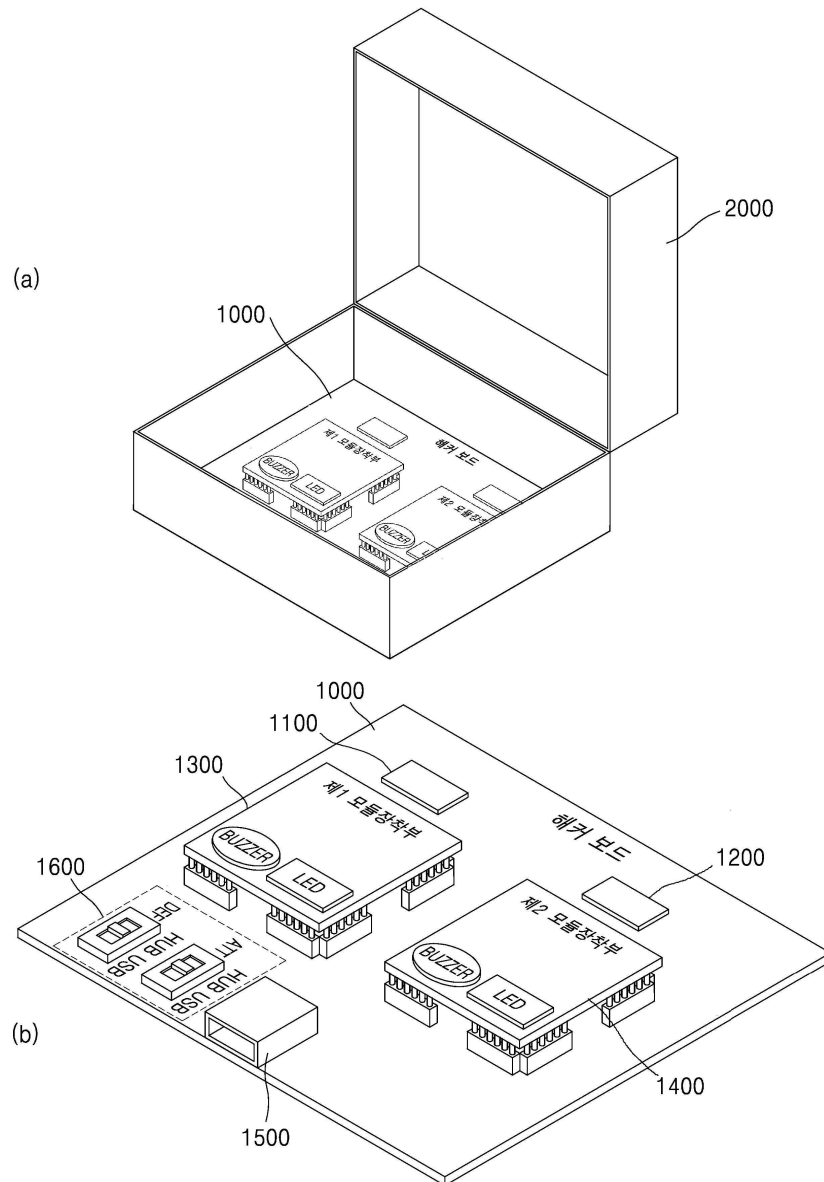
부호의 설명

- [0140] 1000: 해커보드
- 1100: 제1MCU 1200: 제2MCU
- 1300: 제1모듈장착부
- 1310: 제1적외선송신센서 1320: 제1적외선수신센서
- 1330: 제1UART모듈
- 1400: 제2모듈장착부
- 1410: 제2적외선송신센서 1420: 제2적외선수신센서
- 1430: 제2UART모듈
- 1500: USB커넥터 1600: USB스위치모듈
- 1700: UART커넥터 1800: UART스위치모듈

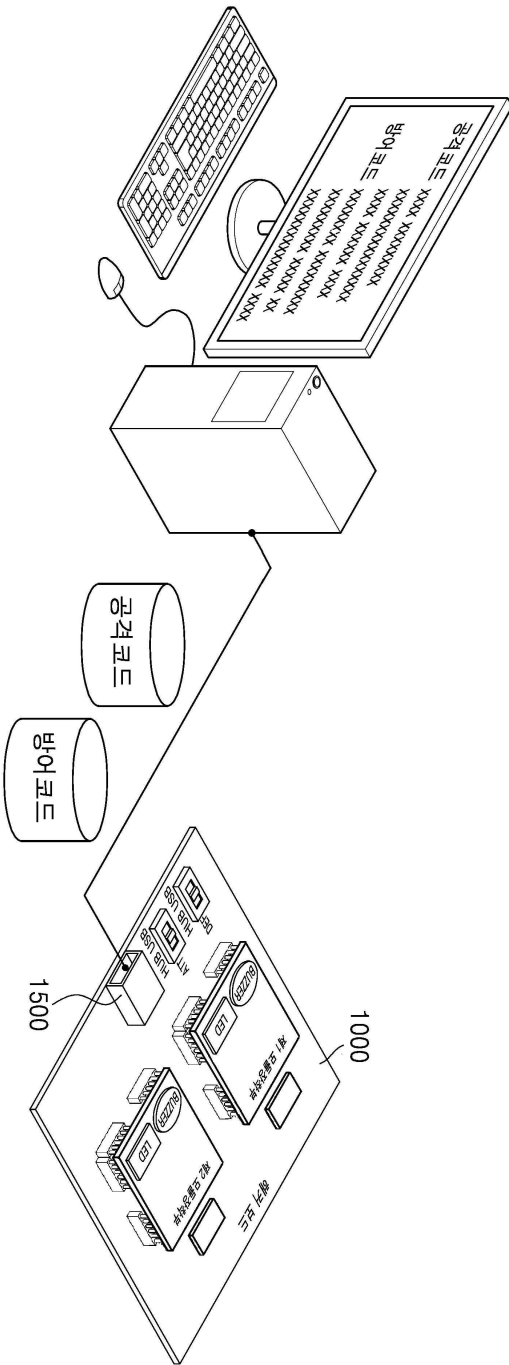
2000: 케이스

도면

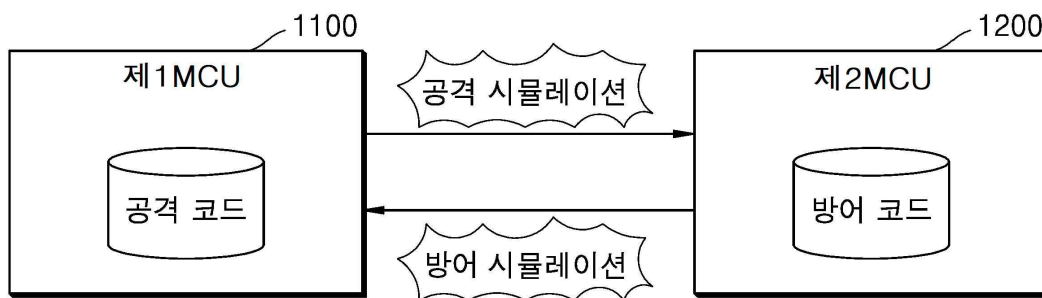
도면1



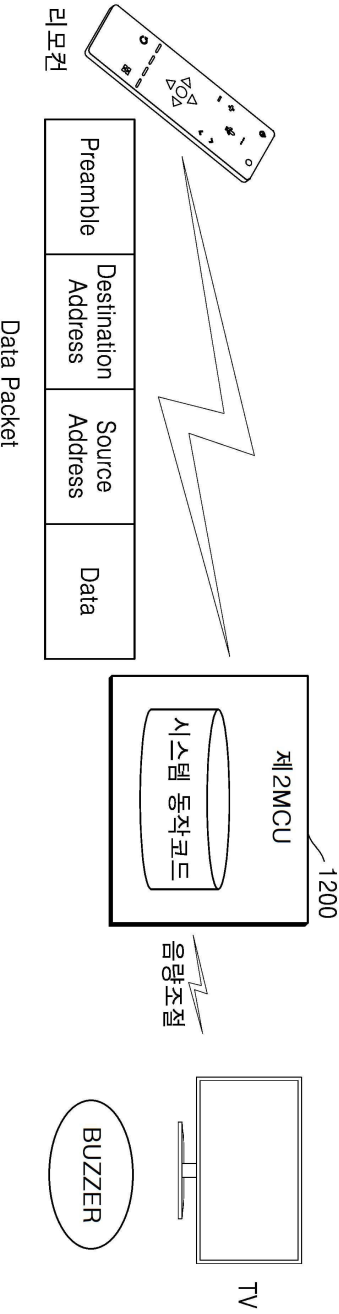
도면2



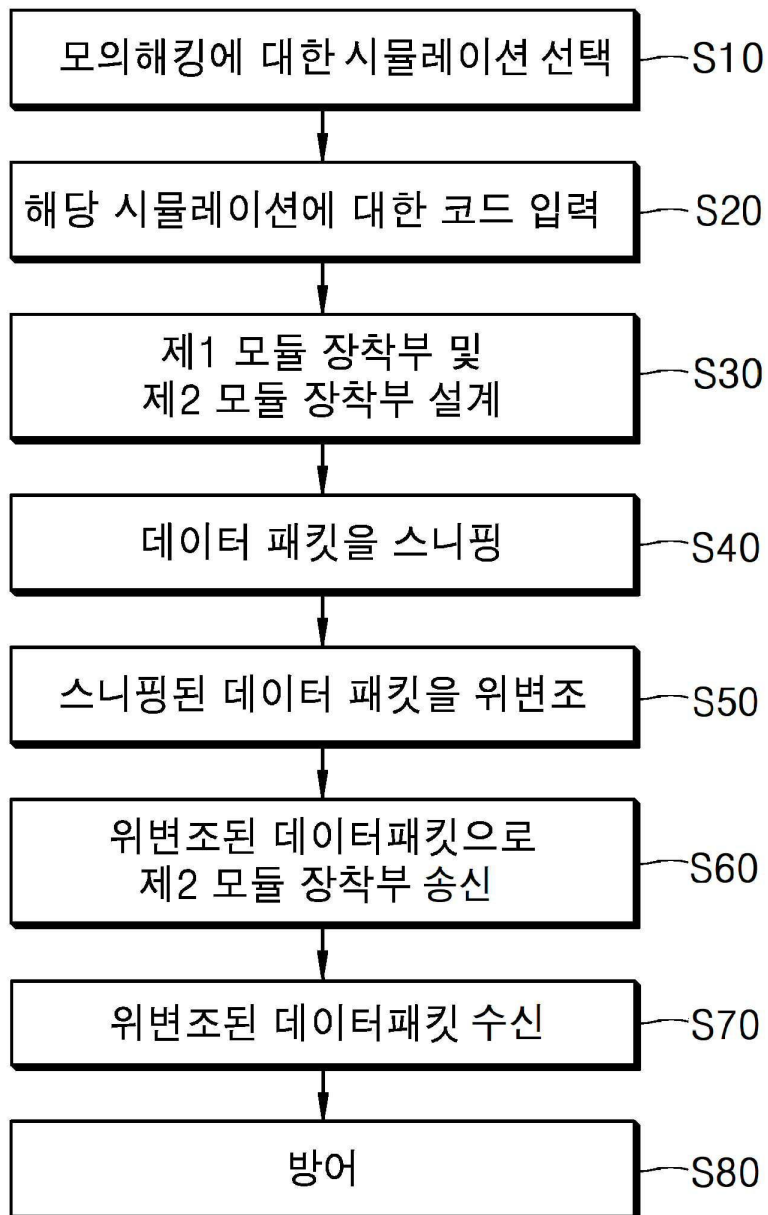
도면3



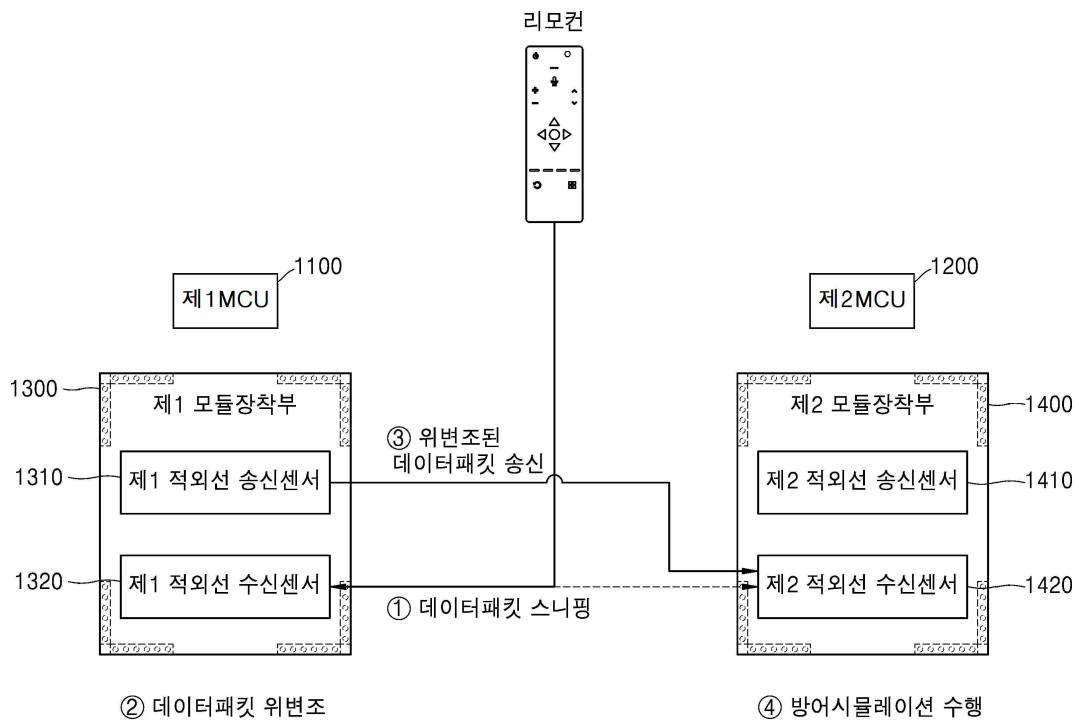
도면4



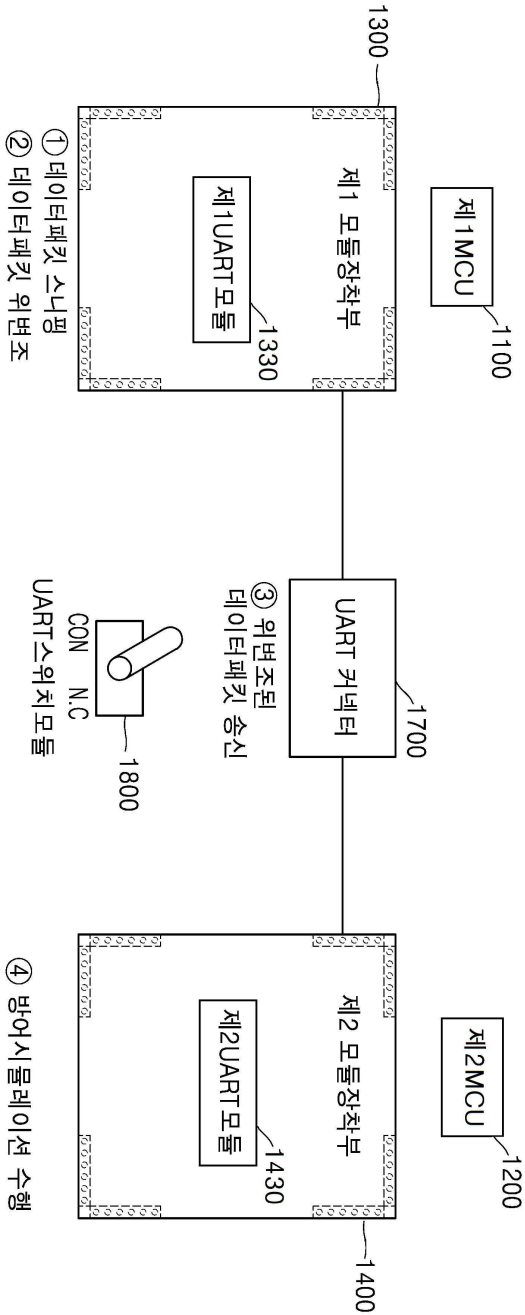
도면5



도면6



도면7



도면8

