(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년03월07일
(11) 등록번호 10-2507499
(24) 등록일자 2023년03월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
H04L 63/145 (2013.01)
(21) 출원번호 10-2022-0059937
(22) 출원일자 2022년05월17일
심사청구일자 2022년05월17일
(56) 선행기술조사문헌
US20200259855 A1*
(뒷면에 계속)

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
송재승
경기도 성남시 분당구 수내로 206, 310동 1001호 (수내동, 푸른마을)
유재훈
경기도 안양시 동안구 관평로212번길 21, 305동 308호(관양동, 공작부영아파트)
(뒷면에 계속)
(74) 대리인
민영준

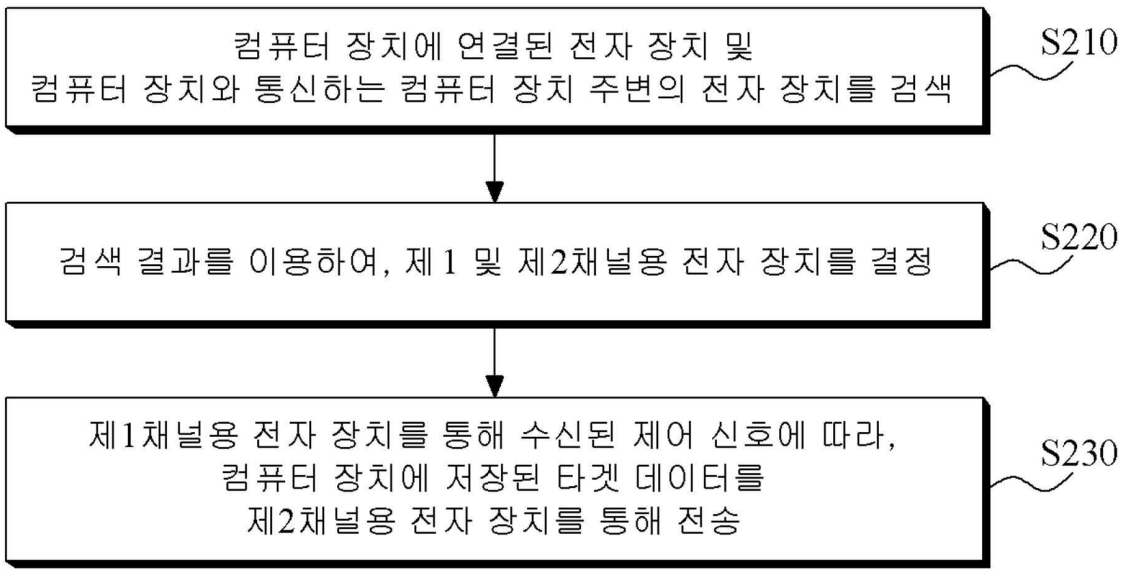
전체 청구항 수 : 총 4 항 심사관 : 정성훈

(54) 발명의 명칭 **양방향 채널을 이용하는 에어갭 환경에서의 공격 방법**

(57) 요 약

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법이 개시된다. 개시된 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법은 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계; 상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및 상기 제1 채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함한다.

대 표 도 - 도2



(72) 발명자

박장용

서울특별시 강동구 상암로 251, 904동 1002호(명일동, 고덕주공아파트)

이영준

서울특별시 종로구 낙산길 198, 206동 1004호(창신동, 창신쌍용아파트 2지구)

이지호

서울특별시 중랑구 동일로92길 40, 108동 1203호(면목동, 사가정 센트럴 아이파크)

(56) 선행기술조사문헌

Mordechai Guri et al., "MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication"(2018.03.)*

Mordechai Guri et al., "aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)"(2017.09.)*

KR1020150120482 A

KR102363559 B1

KR1020210125577 A

*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152732
과제번호	2021-0-01816-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성(R&D)
연구과제명	메타버스 자율트윈 핵심기술 연구
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

컴퓨팅 장치에 의해 수행되는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법에 있어서,

상기 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계;

상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및

상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함하며,

상기 전자 장치를 검색하는 단계는

상기 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 상기 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색하며,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 음향 장치가 상기 제2채널용 전자 장치로 이용되는 상태에서 사람이 상기 음향 장치를 사용하는 경우, 상기 제2채널용 전자 장치를 상기 영상 장치 또는 상기 발광 장치로 변경하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

청구항 2

삭제

청구항 3

제 1항에 있어서,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 음향 장치를 상기 제1채널용 전자 장치로 결정하는,

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

청구항 4

삭제

청구항 5

삭제

청구항 6

컴퓨팅 장치에 의해 수행되는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법에 있어서,

상기 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계;

상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및

상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제

2채널용 전자 장치를 통해 전송하는 단계를 포함하며,

상기 전자 장치를 검색하는 단계는

상기 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 상기 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색하며,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 검색된 전자 장치에 상기 내부 적외선 CCTV가 포함되고, 사람이 상기 컴퓨팅 장치에 근접한 상태이거나, 상기 음향 장치가 사용중인 경우, 상기 컴퓨팅 장치가 배치된 공간의 외부에 위치한 외부 적외선 CCTV를 상기 제1 및 제2채널용 전자 장치로 결정하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

청구항 7

제 1항 또는 제 6항에 있어서,

상기 음향 장치는, 마이크, 스피커, 이어폰 및 헤드폰 중 적어도 하나를 포함하며,

상기 영상 장치는 모니터를 포함하며,

상기 발광 장치는 키보드 램프 및 하드 디스크 램프 중 적어도 하나를 포함하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 에어갭 환경에서의 공격 방법에 관한 것으로서, 더욱 상세하게는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법에 관한 것이다.

배 경 기 술

[0003] 외부 공격으로부터 시스템을 보호하기 위해, 시스템을 네트워크로부터 분리하는 에어갭(air-gapped) 환경이 구축되고 있다. 에어갭 환경에서는 공격자가 네트워크를 통해 시스템에 접근할 수 없으므로, 네트워크를 통해 시스템의 정보를 탈취하는 것은 불가능하다.

[0004] 하지만 최근에는 네트워크를 이용하지 않고, 에어갭 환경의 시스템을 공격하는 시도가 발견되고 있다. 에어갭 환경에서도 시스템은 USB 등을 통해 데이터 탈취를 위한 악성 코드에 감염될 수 있으며, 컴퓨팅 장치의 소리나 광학 신호를 이용하여, 시스템의 정보를 탈취하는 공격 방법이 보고되고 있다.

[0005] 예컨대, 공격자는, 악성 코드를 이용하여, 사용자가 인지할 수 없는 주파수의 소리를 발생시킬 수 있으며, 또는 사용자가 인지할 수 없을 정도로 모니터의 주사율을 변경하거나 컴퓨팅 장치의 LED를 점멸시킬 수 있다. 그리고

공격자는 마이크나 컴퓨팅 장치를 촬영한 영상 또는 광학 신호를 감지하는 포토 다이오드와 같은 광센서를 이용하여, 소리 또는 광학 신호로부터 정보를 탈취할 수 있다.

[0006] 또한 최근에는 기존의 단방향 채널을 이용한 공격 방법에서 더 나아가, 양방향 채널을 이용한 공격 방법에 대한 연구가 이루어지고 있다.

[0007] 관련 선행문헌으로 비특허 문헌인, "MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication, Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici, 2018 IEEE Conference on Dependable and Secure Computing (DSC)", "aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR), Mordechai Guri, Dima Bykhovsky, Yuval Elovici, 2017"가 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법을 제공하기 위한 것이다.

[0010] 특히 본 발명은 컴퓨팅 장치의 주변 환경에 적응적으로 설정된 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0012] 상기한 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계; 상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및 상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함하는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법이 제공된다.

[0013] 또한 상기한 목적을 달성하기 위한 본 발명의 다른 실시예에 따르면, 제1채널용 전자 장치를 통해 제어 신호를 수신하는 단계; 및 악성 코드에 감염된 컴퓨팅 장치에 저장된 타겟 데이터를, 제2채널용 전자 장치를 통해 전송하는 단계를 포함하며, 상기 악성 코드는 상기 컴퓨팅 장치에 연결되거나, 컴퓨팅 장치 주변에서 상기 컴퓨팅 장치와 통신하는 전자 장치 중에서 결정된, 상기 제1 및 제2채널용 전자 장치에 대한 정보를 포함하는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법이 제공된다.

발명의 효과

[0015] 본 발명의 일실시예에 따르면, 데이터의 전송 오류 등이 발생하여 데이터의 재전송이 필요한 상황에서, 양방향 채널을 통해 타겟 데이터의 재전송을 요청할 수 있다.

[0016] 또한 본 발명의 일실시예에 따르면, 컴퓨팅 장치의 주변 환경에 따라 적응적으로 양방향 채널이 설정될 수 있다.

도면의 간단한 설명

[0018] 도 1은 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법의 일예를 설명하기 위한 도면이다.

도 2는 본 발명의 일실시예에 따른 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법을 설명하기 위한 도면이다.

도 3은 본 발명의 다른 실시예에 따른 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0020] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0022] 도 1은 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법의 일예를 설명하기 위한 도면이다.

[0023] 에어갭 환경에서 컴퓨팅 장치에 저장된 데이터를 탈취하기 위한 공격은, 단방향 채널을 이용하는 것이 일반적이다. 단방향 채널이 이용될 경우, 데이터 탈취를 위한 악성 코드에 감염된 컴퓨팅 장치는 데이터 탈취의 대상인 타겟 데이터를 공격자에게 전송할 수 있을 뿐, 공격자로부터 제어 신호를 수신할 수 없다.

[0024] 이에 최근에는 에어갭 환경에서, 양방향 채널을 이용하여 데이터를 탈취할 수 있는 공격 방법이 보고되고 있다. 양방향 채널이 이용될 경우, 악성 코드에 감염된 컴퓨팅 장치는 공격자로부터 제어 신호를 수신하여, 타겟 데이터를 공격자에게 전송할 수 있다. 일예로서, 스피커나 적외선 CCTV 등의 전자 장치들이 양방향 채널로 이용될 수 있다.

[0025] 도 1의 에어갭 환경은, 데이터 탈취의 대상이 되는 타겟 데이터를 저장하고 있는 컴퓨팅 장치(110)와, 적외선 CCTV 네트워크가 외부 통신망과 분리되어 있는 환경이다. 그리고 컴퓨팅 장치(110)는 적외선 CCTV 네트워크에 접속할 수 있는 환경이며, 적외선 CCTV 네트워크에 포함되는 적외선 CCTV는, 컴퓨팅 장치(110)가 존재하는 공간뿐만 아니라, 컴퓨팅 장치(110)가 존재하는 공간의 외부에도 설치되어 있다.

[0026] 이러한 에어갭 환경에서 적외선 CCTV는 양방향 채널로 이용될 수 있다. 공격자(120)는 외부에 설치된 적외선 CCTV(130)를 향해 적외선 LED를 조사하여, 데이터 탈취를 위한 악성 코드에 감염된 컴퓨팅 장치(110)로 타겟 데이터 전송을 요청할 수 있다. 공격자는 타겟 데이터 전송 요청에 대응되는 비트값을, 적외선 LED를 점멸시켜 생성할 수 있으며, 컴퓨팅 장치(110)는 외부에 설치된 적외선 CCTV(130)에 의해 생성된 영상에 포함된 적외선 LED 신호로부터, 타겟 데이터 전송 요청에 대응되는 비트값을 추출하여, 타겟 데이터 전송 요청을 확인할 수 있다. 이와 같이, 적외선 CCTV(130)는 컴퓨팅 장치(110)가 공격자(120)로부터 제어 신호를 수신받는 수신 채널로 이용될 수 있다.

[0027] 또한 적외선 CCTV는 컴퓨팅 장치(110)가 타겟 데이터를 공격자(120)에게 전송하는 전송 채널로 이용될 수 있다. 적외선 CCTV는 적외선 LED를 포함하고 있으며, 컴퓨팅 장치(110)는 타겟 데이터에 대응되는 비트값을, 외부에 설치된 적외선 CCTV(130)에 포함된 적외선 LED를 점멸시켜 공격자(120)에게 전송할 수 있다. 공격자(120)는 점멸되는 적외선 LED 신호를 촬영하거나 적외선 센서를 이용해 적외선 LED 신호를 수신한 후, 촬영된 영상에서 타겟 데이터에 대응되는 비트값을 추출하여 타겟 데이터를 탈취할 수 있다.

[0028] 적외선 CCTV 뿐만 아니라, 스피커나 마이크와 같은 음향 기기 역시 양방향 채널로 이용될 수 있다. 스피커나 마이크는 전기 신호와 사운드를 상호 변환하는 장치로서, 동일한 원리를 이용하고 있기 때문에, 스피커는 마이크로 동작할 수 있으며, 마이크 역시 스피커로 동작할 수 있다.

[0029] 따라서 스피커가 양방향 채널로 이용되는 경우, 공격자는 타겟 데이터 전송 요청을 위한 비트값에 대응되는 주파수의 사운드를 컴퓨팅 장치로 방사하여, 컴퓨팅 장치로 타겟 데이터 전송을 요청할 수 있다. 이 때, 스피커는 마이크로 기능한다. 그리고 컴퓨팅 장치는 타겟 데이터의 비트값에 대응되는 주파수의 사운드를 스피커를 통해 방사하여 공격자에게 타겟 데이터를 전송할 수 있다. 컴퓨팅 장치로 방사되는 사운드 및 컴퓨팅 장치로부터 방사되는 사운드는, 컴퓨팅 장치의 사용자가 인지할 수 없는 고주파의 사운드일 수 있다.

[0030] 이와 같이, 컴퓨팅 장치에 연결된 전자 장치나, 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치가 에어갭 공격을 위한 양방향 채널로 이용될 수 있다. 하지만 양방향 채널로 이용되는 전자 장치들은 컴퓨팅 장치에 항상 연결되어 있지 않을 수 있거나 컴퓨팅 장치 주변에 존재하지 않을 수 있으며, 이러한 상황에서는 양방향 채널을 이용한 공격이 불가능하다.

[0031] 이에 본 발명은, 양방향 채널로 이용될 수 있는 전자 장치를 검색하고, 검색 결과에 따라 양방향 채널로 이용될 수 있는 전자 장치를 결정하여 컴퓨팅 장치의 타겟 데이터를 탈취하는 공격 방법을 제안한다.

[0032] 본 발명의 일실시예에 따른 에어갭 환경에서의 공격 방법은, 탈취 대상인 타겟 데이터를 저장하고 있으며, 메모리 및 프로세서를 포함하는 컴퓨팅 장치에서 수행될 수 있으며, 이러한 컴퓨팅 장치는 공격자에 의해, 데이터 탈취를 위한 악성 코드에 미리 감염된 장치이다.

[0033] 본 발명의 일실시예에 따른 에어갭 환경에서의 공격 방법은, 에어갭 환경에서 수행되는 공격을 탐지하고 방어하는 방법을 개발하는데 이용될 수 있다.

[0035] 도 2는 본 발명의 일실시예에 따른 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법을 설명하기 위한 도면

이다.

[0036] 도 2를 참조하면 본 발명의 일실시예에 따른 컴퓨팅 장치는, 컴퓨팅 장치에 연결된 전자 장치 및 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색(S210)한다. 컴퓨팅 장치는 일실시예로서, 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색할 수 있다. 음향 장치는, 마이크, 스피커, 이어폰 및 헤드폰 중 적어도 하나를 포함할 수 있으며, 영상 장치는 모니터를 포함할 수 있다. 그리고 발광 장치는 키보드 램프 및 하드 디스크 램프 중 적어도 하나를 포함할 수 있다.

[0037] 단계 S210에서 컴퓨팅 장치는, 운영 체제에서 제공하는 주변 장치 검색 기능이나 네트워크 정보를 통해 전자 장치를 검색하거나 또는 컴퓨팅 장치에 대한 영상에서 전자 장치를 검색할 수 있다. 전자 장치 검색에 이용되는 영상은, 컴퓨팅 장치 및 컴퓨팅 장치의 주변이 촬영된 CCTV 영상이거나 또는 컴퓨팅 장치가 촬영한 웹캠 영상일 수 있다. 컴퓨팅 장치는 영상에서, 음향 장치, 영상 장치, 발광 장치 및 적외선 CCTV에 대응되는 객체를 검출함으로써, 컴퓨팅 장치에 연결된 전자 장치 및 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색할 수 있다.

[0038] 컴퓨팅 장치는 단계 S210의 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정(S220)한다. 즉 검색된 전자 장치 중에서, 제1 및 제2채널용 전자 장치가 결정된다. 제1채널은 수신 채널, 제2채널은 전송 채널에 대응된다.

[0039] 음향 장치와 적외선 CCTV는 제1 및 제2채널용 전자 장치로 이용될 수 있으며, 영상 장치 및 발광 장치는 제2채널용 전자 장치로 이용될 수 있다. 예컨대 음향 장치와 영상 장치 및 발광 장치가 검색된 경우, 컴퓨팅 장치는 음향 장치를 제1채널용 전자 장치로 결정하며, 영상 장치 또는 발광 장치를 제2채널용 전자 장치로 결정할 수 있다. 또는 컴퓨팅 장치는 음향 장치만이 검색된 경우, 음향 장치를 제1 및 제2채널용 전자 장치로 결정할 수 있다.

[0040] 또는 검색된 전자 장치에, 컴퓨팅 장치가 배치된 공간에 위치하는 내부 적외선 CCTV가 포함된 경우, 컴퓨팅 장치는, 컴퓨팅 장치가 배치된 공간의 외부에 위치한 외부 적외선 CCTV를 제1 및 제2채널용 전자 장치로 결정할 수 있다. 컴퓨팅 장치는 CCTV 네트워크에 대한 정보를 통해 외부에 위치한 적외선 CCTV를 확인할 수 있다.

[0041] 특히, 영상 장치 및 발광 장치가 제1 및 제2채널용 전자 장치로 이용되는 경우, 사람이 컴퓨팅 장치에 근접한 상태에서 발광 장치의 빛이나, 영상 장치의 깜빡임을 감지하여, 사람에 의해 데이터 유출이 발각될 수 있기 때문에, 컴퓨팅 장치는 사람이 컴퓨팅 장치에 근접한 상태인 경우, 음향 장치나 외부 적외선 CCTV를 제1 및 제2채널용 전자 장치로 결정할 수 있다.

[0042] 또한 사람이 이어폰이나 헤드폰을 착용하여 음향 장치를 사용하는 경우, 음향 장치는 제1 및 제2채널용 전자 장치로 이용될 수 없으므로, 컴퓨팅 장치는 이러한 경우에는 외부 적외선 CCTV를 제1 및 제2채널용 전자 장치로 결정할 수 있다.

[0043] 컴퓨팅 장치는, 컴퓨팅 장치를 촬영하는 CCTV 영상이나, 컴퓨터 장치의 웹캠 영상 등 컴퓨팅 장치에 대한 영상을 이용하여, 사람이 컴퓨팅 장치에 근접한 상태인지 여부 및 사람이 음향 장치를 사용하는지 여부를 판단할 수 있다. 일실시예로서, 영상에서 사람이 컴퓨팅 장치를 미리 설정 시간 동안 가리는 경우, 즉 사람이 미리 설정 시간 동안 컴퓨팅 장치 상에 오버랩된 경우에, 컴퓨팅 장치는, 사람이 컴퓨팅 장치에 근접한 상태인 것으로 판단할 수 있다. 또는 컴퓨팅 장치는, 사람이 컴퓨팅 장치로부터 미리 설정된 거리 내에, 미리 설정된 시간 동안 위치한 경우, 사람이 컴퓨팅 장치에 접근한 상태인 것으로 판단할 수 있다. 또는 사람이 이어폰이나 헤드폰을 착용하고 있는 경우 음향 장치가 사용되고 있는 것으로 판단할 수 있다.

[0044] 또는 음향 장치가 제2채널용 전자 장치로 이용되는 상태에서 사람이 음향 장치를 사용하는 경우, 컴퓨팅 장치는 음향 장치 이외의 전자 장치, 예컨대, 영상 장치나 발광 장치로 제2채널용 전자 장치를 변경할 수 있다.

[0045] 컴퓨팅 장치는 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 컴퓨팅 장치에 저장된 타겟 데이터를 제2채널용 전자 장치를 통해 전송(S230)하며, 제어 신호는 일실시예로서 데이터 전송 요청일 수 있다.

[0046] 음향 장치가 제1채널용 전자 장치로 이용되는 경우, 전술된 바와 같이, 공격자는 타겟 데이터 전송 요청을 위한 비트값에 대응되는 주파수의 사운드를 스피커 등을 이용해 컴퓨팅 장치로 방사하여, 타겟 데이터 전송을 요청할 수 있다. 컴퓨팅 장치는 제1채널용 전자 장치를 이용하여, 방사된 사운드를 수신하고, 타겟 데이터 전송 요청에 응답하여, 제2채널용 전자 장치를 통해 타겟 데이터를 전송할 수 있다.

[0047] 영상 장치 또는 발광 장치가 제2채널용 전자 장치로 이용되는 경우, 컴퓨팅 장치는 모니터의 밝기를 변화시키거나 키보드 또는 하드 디스크의 램프를 점멸시켜, 타겟 데이터에 대응되는 비트값을 생성할 수 있다. 공격자는 포토 다이오드와 같은 광센서를 이용해 타겟 데이터를 수신하거나 또는 컴퓨팅 장치에 대한 영상에서 비트값을 추출할 수 있다.

[0048] 외부 적외선 CCTV가 제1 및 제2채널용 전자 장치로 이용되는 경우, 전술된 바와 같이, 공격자는 적외선 LED를 점멸시켜 타겟 데이터 전송을 요청할 수 있다. 컴퓨팅 장치는 외부 적외선 CCTV의 영상에서 타겟 데이터 전송 요청을 확인하고, 타겟 데이터 전송 요청에 응답하여, 외부 적외선 CCTV를 이용해 타겟 데이터를 전송할 수 있다.

[0049] 공격자는 제2채널용 전자 장치로 이용될 수 있는 전자 장치를 고려하여, 광센서, 적외선 센서, 스피커 등을 이용해, 타겟 데이터를 수신할 수 있다.

[0050] 한편, 컴퓨팅 장치는 제2채널용 전자 장치가 변경되는 경우, 타겟 데이터와 함께 제2채널용 전자 장치의 변경 정보를 공격자에게 전송할 수 있으며, 공격자는 변경된 제2채널용 전자 장치로부터 타겟 데이터를 수신할 수 있다.

[0051] 본 발명의 일실시예에 따르면, 데이터의 전송 오류 등 데이터의 재전송이 필요한 상황에서, 양방향 채널을 통해 타겟 데이터의 재전송을 요청할 수 있다.

[0052] 또한 본 발명의 일실시예에 따르면, 컴퓨팅 장치의 주변 환경에 따라 적응적으로 양방향 채널이 설정될 수 있으며, 다양한 전자 장치를 채널 후보군으로 활용함으로써, 일부 전자 장치의 이용이 어려운 상황에서도 양방향 채널이 설정될 수 있다.

[0054] 도 3은 본 발명의 다른 실시예에 따른 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법을 설명하기 위한 도면이다.

[0055] 공격자는 컴퓨팅 장치에 연결되거나 컴퓨팅 장치 주변에서 컴퓨팅 장치와 통신하는 전자 장치를 확인하고, 확인된 전자 장치 중에서 제1 및 제2채널용 전자 장치를 결정(S310)할 수 있다. 공격자는 컴퓨팅 장치 및 컴퓨팅 장치의 주변을 촬영한 영상 또는 컴퓨팅 장치에서 촬영된 영상으로부터 제1 및 제2채널용 전자 장치를 결정할 수 있다.

[0056] 일실시예로서, 컴퓨팅 장치에 연결된 음향 장치, 영상 장치 및 발광 장치가 확인된 경우, 제1채널용 전자 장치는 컴퓨팅 장치에 연결된 음향 장치로 결정될 수 있으며, 제2채널용 전자 장치는 영상 장치 및 발광 장치 중 하나로 결정될 수 있다.

[0057] 또는 컴퓨팅 장치와 통신하는 전자 장치 중 상기 컴퓨팅 장치 주변에 위치하는 내부 적외선 CCTV가 존재하는 경우, 컴퓨팅 장치가 설치된 공간의 외부에 위치한 외부 적외선 CCTV가 제1 및 제2채널용 전자 장치로 결정될 수 있다.

[0058] 그리고 공격자는 제1 및 제2채널용 전자 장치에 대한 정보를 포함하는, 데이터 유출을 위한 악성 코드를 제작(S320) 및 유포(S330)하여 컴퓨팅 장치를 감염(S340)시킬 수 있다.

[0059] 공격자는 악성 코드에 감염된 컴퓨팅 장치로 제1채널용 전자 장치를 통해 제어 신호를 전송(S350)하고, 컴퓨팅 장치는 제1채널용 전자 장치를 통해 수신(S360)한다. 그리고 컴퓨팅 장치는 제어 신호에 응답하여 컴퓨팅 장치에 저장된 타겟 데이터를, 제2채널용 전자 장치를 통해 전송(S370)한다. 제어 신호는 일실시예로서, 데이터 전송 요청일 수 있다.

[0060] 공격자는 미리 결정된 제2채널용 전자 장치에 대응하여, 타겟 데이터를 수신할 수 있다. 예컨대, 제2채널용 전자 장치가 발광 장치라면, 광센서를 이용해 타겟 데이터를 수신할 수 있으며, 제2채널용 전자 장치가 외부 적외선 CCTV라면, 외부 적외선 CCTV에서 적외선 센서를 이용해 타겟 데이터를 수신할 수 있다.

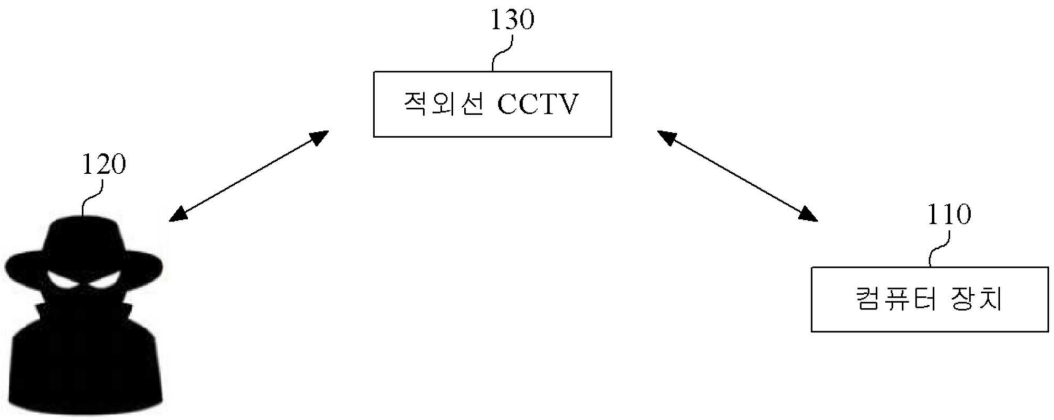
[0062] 앞서 설명한 기술적 내용들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예들을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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. 하드웨어 장치는 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

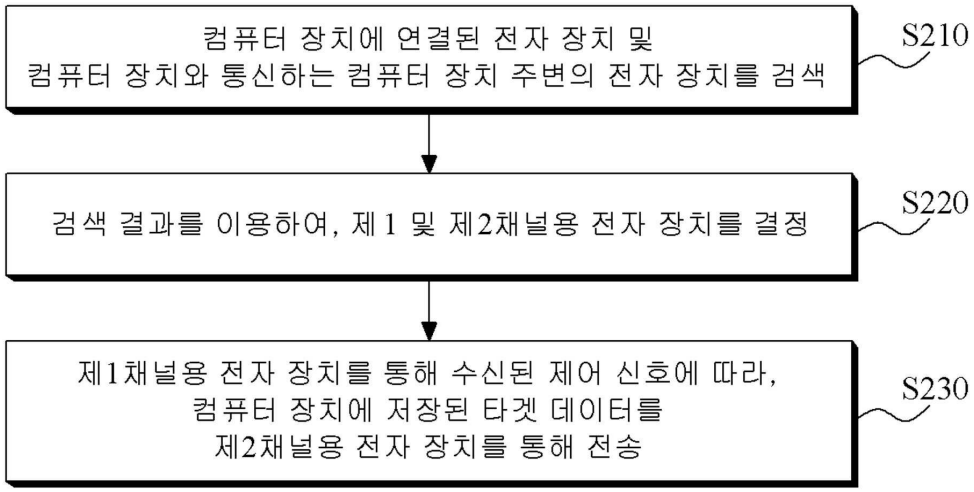
[0064] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

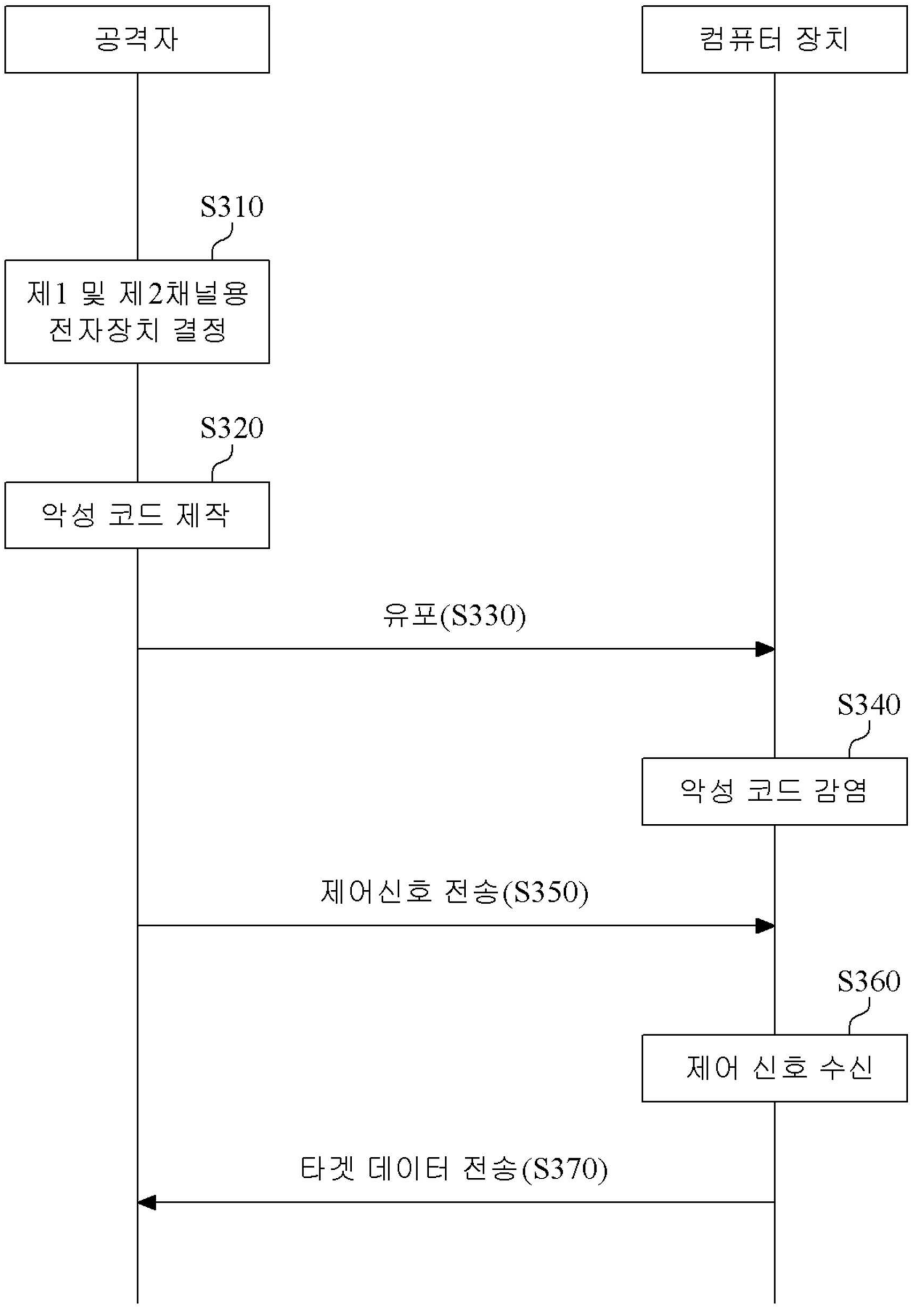
도면1



도면2



도면3



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 1

【변경전】

컴퓨팅 장치에 의해 수행되는 에어갭 환경에서의 공격 방법에 있어서,

상기 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계;

상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및

상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함하며,

상기 전자 장치를 검색하는 단계는

상기 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 상기 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색하며,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 음향 장치가 상기 제2채널용 전자 장치로 이용되는 상태에서 사람이 상기 음향 장치를 사용하는 경우, 상기 제2채널용 전자 장치를 상기 영상 장치 또는 상기 발광 장치로 변경하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

【변경후】

컴퓨팅 장치에 의해 수행되는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법에 있어서,

상기 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계;

상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및

상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함하며,

상기 전자 장치를 검색하는 단계는

상기 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 상기 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색하며,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 음향 장치가 상기 제2채널용 전자 장치로 이용되는 상태에서 사람이 상기 음향 장치를 사용하는 경우, 상기 제2채널용 전자 장치를 상기 영상 장치 또는 상기 발광 장치로 변경하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

【직권보정 2】

【보정항목】청구범위

【보정세부항목】청구항 6

【변경전】

컴퓨팅 장치에 의해 수행되는 에어갭 환경에서의 공격 방법에 있어서,

상기 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계;

상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및

상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함하며,

상기 전자 장치를 검색하는 단계는

상기 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 상기 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색하며,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 검색된 전자 장치에 상기 내부 적외선 CCTV가 포함되고, 사람이 상기 컴퓨팅 장치에 근접한 상태이거나, 상기 음향 장치가 사용중인 경우, 상기 컴퓨팅 장치가 배치된 공간의 외부에 위치한 외부 적외선 CCTV를 상기 제1 및 제2채널용 전자 장치로 결정하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.

【변경후】

컴퓨팅 장치에 의해 수행되는 양방향 채널을 이용하는 에어갭 환경에서의 공격 방법에 있어서,

상기 컴퓨팅 장치에 연결된 전자 장치 및 상기 컴퓨팅 장치와 통신하는 컴퓨팅 장치 주변의 전자 장치를 검색하는 단계;

상기 검색 결과를 이용하여, 제1 및 제2채널용 전자 장치를 결정하는 단계; 및

상기 제1채널용 전자 장치를 통해 수신된 제어 신호에 따라, 상기 컴퓨팅 장치에 저장된 타겟 데이터를 상기 제2채널용 전자 장치를 통해 전송하는 단계를 포함하며,

상기 전자 장치를 검색하는 단계는

상기 컴퓨팅 장치에 연결된 음향 장치, 영상 장치, 발광 장치 및 상기 컴퓨팅 장치 주변의 내부 적외선 CCTV를 검색하며,

상기 제1 및 제2채널용 전자 장치를 결정하는 단계는

상기 검색된 전자 장치에 상기 내부 적외선 CCTV가 포함되고, 사람이 상기 컴퓨팅 장치에 근접한 상태이거나, 상기 음향 장치가 사용중인 경우, 상기 컴퓨팅 장치가 배치된 공간의 외부에 위치한 외부 적외선 CCTV를 상기 제1 및 제2채널용 전자 장치로 결정하는

양방향 채널을 이용하는 에어갭 환경에서의 공격 방법.