



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월05일
(11) 등록번호 10-1426926
(24) 등록일자 2014년07월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
(21) 출원번호 10-2013-0010609
(22) 출원일자 2013년01월30일
심사청구일자 2013년01월30일
(56) 선행기술조사문헌
'무선 USB 정보보안', 정보통신단체표준(TTAS),
표준번호: TTAK.OT-06.0033, 2009.09.23.
KR100759168 B1
KR1020110122432 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
최진영
서울 노원구 동일로248길 16, 506동 1003호 (상계
동, 수락파크빌)
강미영
서울 성북구 아리랑로 89, 110동 1102호 (돈암동,
일신건영휴먼빌아파트)
민소라
서울 성북구 안암로 145, 융합소프트웨어전문대학
원 (안암동5가, 고려대학교)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 5 항

심사관 : 이병수

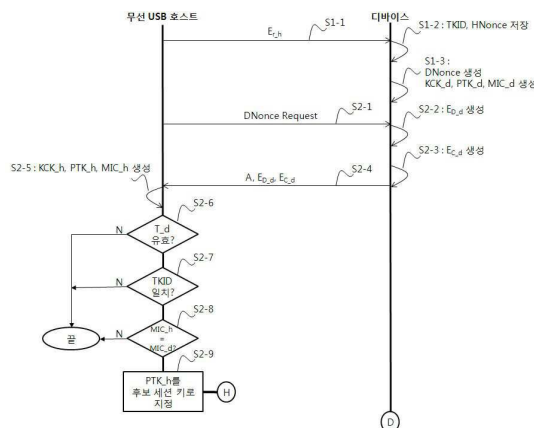
(54) 발명의 명칭 무선 USB 호스트와 디바이스 간 통신 채널 설정 방법

(57) 요약

본 발명은 무선 USB(Wireless Universal Serial Bus: WUSB) 호스트와 디바이스 간에 통신 세션(session)동안 사용될 통신 채널을 설정함에 있어 외부로부터의 공격에 안전하도록 통신 채널을 설정하는 방법에 관한 것이며, 특히 무선 USB 호스트와 디바이스 간의 상기한 통신 채널 설정에 요구되는 호스트와 디바이스 간 상호 인증(mutual authentication) 과정에서 발생할 수 있는 외부로부터의 공격에 안전성(security)을 확보할 수 있는 통신 채널 설정 방법에 관한 것이다.

개시되는 통신 채널 설정 방법은 무선 USB 호스트와 디바이스 간에 소정의 통신 세션동안 사용될 통신 채널을 설정함에 전제되는 상기 호스트와 상기 디바이스 간 상호 인증에 요구되는 값(메시지)들이 상기 호스트와 상기 디바이스에 의해 각각 암호화되어 상호 교환되며, 상기 각각의 암호화를 위한 암호화 키는 상기 호스트와 상기 디바이스 간에는 서로 교환되지 아니하고 상기 호스트와 상기 디바이스 각자에 저장되며, 상기 세션동안 사용될 세션 키(session key)는 상기 호스트와 상기 디바이스에 각각 예비적으로 생성되며, 상기 생성된 각 세션 키는 상기 호스트와 상기 디바이스 간에 서로 교환되지 아니하고 상기 암호화되어 상호 교환되는 값들을 근거로 확정되어 상기 호스트와 상기 디바이스 각자에 저장되도록 하여 본 발명의 과제를 해결한다.

대표도 - 도2a



특허청구의 범위

청구항 1

무선 USB(Wireless USB) 호스트와 디바이스 간에 소정의 통신 세션(session)동안 사용될 통신 채널을 설정함에 전제되는 상기 호스트와 상기 디바이스 간 상호 인증(mutual authentication)에 요구되는 값(메시지)들이 상기 호스트와 상기 디바이스에 의해 각각 암호화되어 상호 교환되며,

상기 각각의 암호화를 위한 암호화 키는 상기 호스트와 상기 디바이스 간에는 서로 교환되지 아니하고 상기 호스트와 상기 디바이스 각자에 저장되며,

상기 통신 세션동안 사용될 세션 키(session key)는 상기 호스트와 상기 디바이스에 각각 예비적으로 생성되며, 상기 생성된 각 세션 키는 상기 호스트와 상기 디바이스 간에 서로 교환되지 아니하고 상기 암호화되어 상호 교환되는 값들을 근거로 최종 확정되어 상기 호스트와 상기 디바이스 각자에 저장되는 것을 특징으로 하며,

a) WUSB 규격에 의한 Connection Context(CC)가 상기 디바이스에 분배된 후 상기 디바이스가 상기 호스트에 상기 통신 채널의 설정을 요청하면, 상기 호스트가 상기 디바이스를 식별하기 위한 메시지를 전송하고 상기 디바이스가 이를 수신하는 단계;

b) 상기 호스트가 상기 디바이스가 상기 통신 채널을 설정할 수 있는 정당한 자격이 있는지를 상기 전송된 메시지에 대한 상기 디바이스로부터의 응답 메시지를 근거로 하여 예비적으로 판단하는 단계; 및

c) 상기 디바이스가 상기 호스트의 상기 b) 단계에 의한 판단 결과를 반영한 메시지를 전송받아 이를 근거로 상기 호스트가 상기 통신 채널을 설정할 수 있는 정당한 상대방인지 판단하고, 이 판단 결과에 따라 상기 예비적으로 생성되었던 각 세션 키가 상기 호스트와 상기 디바이스에 각각 최종적으로 구축되는지 여부가 결정되는 단계를 포함하는 것을 특징으로 하고,

상기 a) 단계는

a1) 상기 호스트가 상기 디바이스를 식별하기 위한 키(TKID)를 디피-헬만 알고리즘을 통해 암호화한 메시지를 상기 디바이스에 전송하는 단계;

a2) 상기 디바이스가 상기 암호화된 TKID(Temporal Key ID)를 복호화하여 저장하는 단계; 및

a3) 상기 디바이스가 상기 TKID를 유사난수생성(pseudo random number generation)함수에 적용하여 상기 통신 세션에 사용될 자신의 세션 키(PTK_d)를 생성하여 저장하는 단계를 포함하는 것을 특징으로 하는 무선 USB 호스트와 디바이스 간 통신 채널 설정 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제 1 항에 있어서, 상기 b) 단계는

b1) 상기 디바이스가 상기 TKID와 타임 스탬프(time stamp)를 디피-헬만 알고리즘을 통해 암호화한 메시지를 상기 호스트에 전송하는 단계;

b2) 상기 호스트가 상기 TKID를 유사난수 생성함수에 적용하여 상기 세션에 사용될 자신의 세션 키(PTK_h)를 생성하는 단계;

b3) 상기 호스트가 상기 타임 스탬프의 유효 여부를 판단하여, 유효하다면 상기 디바이스로부터 받은 TKID와 자신이 상기 a1) 단계에 의해 상기 디바이스에 전송한 TKID가 일치하는지 판단하는 단계; 및

b4) 상기 타임 스탬프가 유효하고 아울러 상기 두 TKID가 일치하는 경우, 상기 호스트가 상기 PTK_h를 상기 세

선에 이용될 자신의 후보 세션 키로 지정하는 단계를 포함하는 것을 특징으로 하는 무선 USB 호스트와 디바이스 간 통신 채널 설정 방법.

청구항 5

제 4 항에 있어서, 상기 c) 단계는

c1) 상기 호스트가 상기 TKID와 상기 타임 스탬프에 대응하는 또 다른 타임 스탬프를 암호화한 메시지(C1)를 상기 디바이스에 전송하는 단계;

c2) 상기 디바이스가 상기 암호화한 메시지(C1)가 유효하다고 판단하면 상기 a3) 단계에서 생성한 PTK_d를 상기 세션에 이용할 자신의 세션 키로 확정하여 저장하고, 상기 호스트에 상기 PTK_d의 확정을 통지하는 단계; 및

c3) 상기 호스트가 상기 통지를 받으면 상기 PTK_h를 상기 세션에 이용할 자신의 세션 키로 확정하여 저장하는 단계를 포함하되,

상기 c2) 단계는

상기 디바이스가 상기 암호화한 메시지(C1)가 유효하지 않는다고 판단하면 상호 인증 과정을 진행하지 않고, 상기 상호 인증 과정을 진행하지 않는다는 사실을 상기 호스트로 통지하는 것을 특징으로 하는 무선 USB 호스트와 디바이스 간 통신 채널 설정 방법.

청구항 6

제 1 항 또는 제 4 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 저장은 상기 각자의 스마트카드(smart card)에 이루어지는 것을 특징으로 하는 무선 USB 호스트와 디바이스 간 통신 채널 설정 방법.

청구항 7

제 1 항 또는 제 4 항 내지 제 5 항 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체.

명세서

기술분야

[0001] 본 발명은 무선 USB 호스트와 디바이스 간 통신 채널 설정 방법에 관한 것으로, 보다 상세하게는 무선 USB(Wireless Universal Serial Bus: WUSB) 호스트와 디바이스 간에 통신 세션(session)동안 사용될 통신 채널을 설정함에 있어 외부로부터의 공격에 안전하도록 통신 채널을 설정하는 방법에 관한 것이며, 특히 무선 USB 호스트와 디바이스 간의 상기한 통신 채널 설정에 요구되는 호스트와 디바이스 간 상호 인증(mutual authentication) 과정에서 발생할 수 있는 외부로부터의 공격에 안전성(security)을 확보할 수 있는 통신 채널 설정 방법에 관한 것이다.

배경기술

[0002] 컴퓨터와 주변 장치를 연결해주는 USB(Universal Serial Bus)가 발표된 이후, USB의 사용이 일반화되고 무선 랜의 보급이 확대되면서 USB를 무선으로 지원하는 무선 USB가 등장하게 되었다.

[0003] 도 1은 무선 USB가 적용될 수 있는 컴퓨팅 환경을 제시한 도면이다.

[0004] 도 1을 참조하면, 무선 USB가 적용되는 컴퓨팅 환경은 무선 USB 호스트로서의 기능을 수행하는 호스트 컴퓨터(2)와 호스트 컴퓨터(2)와 무선 USB를 통해 통신 세션이 설정되어 호스트 컴퓨터(2)에 연결되는 디바이스(31~34)로 구성된다. 디바이스(31~34)는 예를 들면 WUSB 키보드, 프린터, 외부 저장 장치, 디지털 카메라 등이 그 예이며 호스트 컴퓨터(2)에 계속적으로 접속하거나 임시적으로 접속할 수 있다.

[0005] 무선 USB 호스트(호스트 컴퓨터, 이하 '호스트'로 약칭)와 디바이스는 서로 간에 어느 하나의 통신 세션동안 사용될 통신 채널을 설정하기 위해 상호 인증 과정이 선행적으로 요구된다. 이러한 상호 인증 과정이 수행되는 동안에는 호스트와 디바이스 간에 여러 메시지(상호 인증에 요구되는 여러 값)가 교환되는데, 기존의 무선 USB가

적용되는 환경에서는 상호 인증 과정이 진행되는 동안에 서로 교환되는 메시지가 외부 공격자에게 쉽게 노출되어 메시지의 무결성(integrity)이 훼손되거나 외부로부터의 도청 내지는 변조가 가능하여 보안상의 위협도가 매우 높은 실정이다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상기한 실정을 감안하여 창안된 것으로, 본 발명이 해결하고자 하는 과제는 호스트와 디바이스 간의 통신 채널의 설정에 요구되는 상호 인증 과정의 진행 중에 서로 교환되는 메시지에 대한 보안상의 위협을 제거하여 호스트와 디바이스 간의 통신 채널을 설정하는 과정에서 발생할 수 있는 외부 공격자로부터의 위협에 대한 안전성(보안성)을 확보할 수 있는 통신 채널을 설정하는 방법을 제시하는 것이다.

과제의 해결 수단

[0007] 상기와 같은 과제를 해결하기 위해 개시되는 통신 채널의 설정 방법은 무선 USB(Wireless USB) 호스트와 상기 호스트와의 통신 세션(session)동안 사용될 통신 채널의 설정을 요청한 디바이스 간에 상기 통신 채널을 설정함에 전제되는 상호 인증(mutual authentication)에 요구되는 값(메시지)들이 상기 호스트와 상기 디바이스에 의해 각각 암호화되어 상호 교환되도록 한다.

[0008] 이때, 상기 각각의 암호화를 위한 암호화 키는 상기 호스트와 상기 디바이스 간에는 서로 교환되지 아니하고, 상기 호스트와 상기 디바이스 각자에 저장되도록 함이 상기한 과제를 해결하기 위해 바람직하다. 아울러 상기 통신 세션동안 사용될 세션 키는 상기 호스트와 상기 디바이스에 각각 예비적으로 생성되며, 상기 생성된 각 세션 키는 상기 호스트와 상기 디바이스 간에 서로 교환되지 아니하고 상기 암호화되어 상호 교환되는 값들을 근거로 확정되도록 하는 것이 상기한 과제를 해결하기 위해 바람직하다.

발명의 효과

[0009] 본 발명은 호스트와 디바이스 간의 통신 세션동안 사용될 통신 채널의 설정에 요구되는 상호 인증 과정의 진행 중에 서로 교환되는 메시지의 암호화에 필요한 암호화 키를 상호 교환하지 아니하도록 하기 때문에 호스트와 디바이스 간의 통신 채널을 설정하는 과정에서 발생할 수 있는 외부 공격자로부터의 위협에 대한 안전성(보안성)을 확보할 수 있다.

[0010] 아울러 통신 세션동안 사용될 각자의 세션 키(session key)도 상호 교환하는 것이 아니라 상기한 서로 교환되는 암호화된 메시지를 통해 통신 세션동안 사용될 각자의 세션 키를 미리 지정(생성)한 후 상기한 암호화된 메시지에 포함된 다른 값의 유효성 체크 내지는 소정 값의 일치 여부를 통해 최종 확정하므로 이에 의해서도 안전성을 보장할 수 있다.

[0011] 아울러 상기한 암호화 키, 세션 키를 각자의 스마트카드에 저장함으로써 tamper-resistance를 도모할 수 있기 때문에 안전성의 보장이 가일층 확보될 수 있다.

도면의 간단한 설명

[0012] 도 1은 무선 USB가 적용될 수 있는 컴퓨팅 환경을 제시한 도면이다.

도 2a 내지 도 2b는 본 발명의 흐름을 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 발명을 실시하기 위한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하려는 과제의 해결방안의 개요를 우선 제시한다.

[0014] 무선 USB가 적용되는 환경에서 상기한 보안상의 위협도가 매우 높은 현 실정을 감안하여, 본 발명은 호스트와 디바이스 간의 통신 세션동안 사용될 통신 채널의 설정에 요구되는 상호 인증 과정의 진행 중에 서로 교환되는 메시지(상호 인증에 요구되는 값)를 '암호화'하여 교환되도록 한다. 이에 덧붙여 본 발명은 보안성의 한층 강화를 위해 호스트와 디바이스는 상기한 서로 교환되는 메시지의 암호화에 필요한 암호화 키를 상호 교환하지 아니하도록 하며, 아울러 통신 세션동안 사용될 각자의 세션 키(session key)를 상호 교환하는 것이 아니라 상기한 서로 교환되는 암호화된 메시지를 통해 통신 세션동안 사용될 각자의 세션 키를 미리 지정(생성)한 후 상기한

암호화된 메시지에 포함된 다른 값의 유효성 체크 내지는 소정 값의 일치 여부를 통해 최종 확정하도록 한다. 이러한 교환을 생략시켜 버리면 외부에 의해 암호화 메시지 해독의 전제가 되는 키들을 추출하는 것이 원천적으로 불가능하므로 안전성 보장을 확실히 할 수 있다.

[0015] 그리고 상호 인증 과정 시 요구되는 호스트와 디바이스에서 생성되는 여러 값과 암호화 키, 세션 키를 각자의 스마트카드(smart card)에 저장하여 tamper-resistance를 도모한다.

[0016] 이하, 본 발명을 실시하기 위한 구체적인 내용을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면 상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0017] 우선 설명의 편의를 위해 본 발명이 구현되는 과정에서 요구되는 제반 값 내지는 키의 의미를 아래 도표로 선행 제시한다.

표 1

[0018]	내 용
HNonce	호스트가 생성한 128bit 랜덤 nonce 값.
DNonce	디바이스가 생성한 128bit 랜덤 nonce 값.
TKID	Temporal Key ID로서 호스트가 통신 채널 설정 요청을 한 디바이스를 식별하기 위한 키. PTK(Pair Temporal Key)와 GTK(Group Temporal Key)를 위한 이름. GTK는 PTK가 생성된 후 생성되는 것으로 특정 네트워크에 속해 있는 모든 디바이스는 같은 GTK를 갖게 되며, 호스트는 이 키를 이용하여 특정 네트워크에 속한 모드 디바이스에게 소정의 메시지를 브로드캐스트 할 수 있음.
KCK_h (KCK_d)	호스트(디바이스)가 생성하는 Key confirmation Key. 인증 과정에서만 사용되는 short-term 키 값
PTK_h (PTK_d)	호스트(디바이스)가 생성하는 Pair Temporal Key로서, 이 키가 바로 상호 인증 과정에 의해 호스트(디바이스)에 생성되는 세션 키(session key)이다.
MIC_h (MIC_d)	호스트(디바이스)가 생성하는 Message Integrity code로, 상호 교환되는 암호화 메시지의 무결성을 보장하기 위한 코드.
r_h	호스트에서 생성하는 랜덤 값.
r_d	디바이스에서 생성하는 랜덤 값.
{E _x }	x를 암호화 키로 하여 E를 암호화한 메시지
{E _x } ⁻¹	E _x 를 복호화한 메시지
D_d	Diffie-Hellman 알고리즘에 의해 생성된 연결 키(CK)를 디바이스가 해시(hash)한 값
D_h	Diffie-Hellman에 알고리즘에 의해 생성된 연결 키(CK)를 호스트가 해시한 값
h(a)	a의 단방향 해시 값(unilateral hashed value)
	스트링 결합(concatenation)

[0019] 위의 도표에서 _h는 호스트(2)에 의함임을 나타내는 것이며 이하 같다. 아울러 상대적으로 _d는 디바이스에 의함임을 나타내는 것이다.

[0020] 본 발명에 의한 상호 인증 과정의 구현에 앞서 Connection Context(CC)가 호스트(2)에 의해 디바이스에 분배된다. 분배는 WUSB 규격에 의한다. CC는 각각 128 bit의 크기를 갖는 호스트 ID인 CHID(Connection Host ID), 디바이스 ID인 CDID(Connection Device ID) 및 연결 키 CK(Connection Key)로 구성된다. 본 발명에서 CC는 호스트(2)와 디바이스의 안전한 연결을 위해서 외부 공격에 둔감한 Out-Of-Band(OOB) 채널을 통해 분배되며, CC에 포함되는 CK는 디피-헬만(Diffie-Hellman) 암호화 알고리즘(이하 'DH 알고리즘')을 기반으로 하는 공개키 교환 방식으로 디바이스에 분배된다. 다만, 암호화 알고리즘은 반드시 DH 알고리즘으로만 국한되는 것은 아니며 제반 상황을 고려하여 다른 암호화 알고리즘의 적용도 가능하다.

[0021] CC의 분배가 완료된 후 디바이스가 CDID를 호스트(2)에 제공하여 호스트(2)와의 통신 채널 설정을 요청하면, 호스트(2)와 디바이스에서는 각각 상호 인증을 수행하기 위한(안전한 통신 채널을 설정하기 위한) 사전 작업이 진

행된다. 사전 작업은 구체적으로 다음과 같이 진행된다.

- [0022] 호스트(2)는 랜덤 값 r_h , b , p , g 를 생성한다. r_h 는 128 bit의 키이며, b , p , g 는 DH 알고리즘에서 사용하기 위한 소수(prime number)이다. 호스트(2)는 디바이스에 r_h , b , p , g , $B [= g^b \bmod p]$ 를 전송한다. 호스트(2)로부터 r_h , b , p , g , B 를 전송받은 디바이스는 이들 값을 자신의 스마트카드에 저장한 후 랜덤 값 a 를 생성하여 DH 알고리즘을 사용하여 $A [= g^a \bmod p]$ 를 계산한다.
- [0023] 호스트(2)와 디바이스는 상기한 사전 작업이 완료된 이후에 4개의 메시지 교환을 통해 각자의 세션 키를 생성하는 데, 이를 위한 4개의 메시지 교환 프로토콜을 4-way handshake라 한다. 4-way handshake에 관한 상세는 WUSB 규격에 제시되어 있으며, 본 발명에 의한 상호 인증 과정은 4-way handshake에 기반을 둔다.
- [0024] 우선 상호 인증 과정(4-way handshake)의 첫 번째 단계(S1)로, 본 단계는 호스트(2)가 자신에게 소정의 세션동안 사용될 통신 채널 설정 요청을 한 디바이스를 식별하기 위한 사전 단계이다. 본 단계(S1)는 아래와 같이 S1-1 내지 S1-3 단계로 구현된다.
- [0025] 호스트(2)는 TKID와 HNonce를 생성하고 이들을 암호화한 메시지 E_{r_h} 를 디바이스에 전송한다(S1-1). 디바이스는 E_{r_h} 를 복호화하여 호스트(2)로부터 전송받은 TKID와 HNonce를 추출하여 자신의 스마트카드에 저장한다(S1-2). 이때 E_{r_h} 는 $\{TKID || HNonce\}$ 를 r_h 를 암호화 키로 하여 DH 알고리즘에 의해 암호화하여 생성될 수 있다($E_{r_h} = \{TKID || HNonce\}_{r_h}$). 디바이스는 DNonce를 생성하고 HNonce와 DNonce를 이용하여 KCK_d, PTK_d, MIC_d를 생성한다(S1-3). KCK_d, PTK_d, MIC_d는, 예를 들어, HNonce와 DNonce를 생성 파라미터로 하는 pseudo random number generation 함수(PTF)를 사용하여 생성할 수 있다.
- [0026] 다음으로 상호 인증 과정(4-way handshake)의 두 번째 단계(S2)로, 본 단계는 호스트(2)가 자신에게 통신 채널 설정 요청을 한 디바이스가 통신 채널을 설정할 수 있는 정당한 자격을 갖는지 예비적으로 판단하기 위한 단계이다. 본 단계(S2)는 아래와 같이 S2-1 내지 S2-9 단계로 구현된다.
- [0027] 호스트(2)는 자신과의 통신 채널 설정을 요청한 디바이스에 DNonce의 전송 요청 메시지(DNonce Request Message)를 전송한다(S2-1). 이는 호스트가 디바이스에 의해 상기한 TKID가 수신되었는지 확인하고 아울러 디바이스에서 생성된 세션 키(PTK_d)에 대응하는 세션 키(PTK_h)를 생성하기 위한 사전 작업으로 볼 수 있다.
- [0028] DNonce의 전송 요청을 받은 디바이스는 호스트(2)로부터 사전에 전달받은 B 를 이용하여 $D_d [= h(B^a \bmod p)]$ 를 생성한다. 그 후 디바이스는 D_d 를 암호화 키로 하여 암호화된 메시지 $E_{D_d} [= (TKID || DNonce || T_d)_{D_d}]$ 를 생성한 다음(S2-2), $C_d [= h(DNonce) (+) D_d]$ 를 암호화 키로 하여 암호화된 메시지 $E_{C_d} [= (TKID || MIC_d)_{C_d}]$ 를 생성한다(S2-3). 디바이스는 A , E_{D_d} , E_{C_d} 를 호스트(2)에게 전송한다(S2-4). 여기서 (+)는 배타적 논리합 연산을 의미하며, T_d 는 타임 스탬프(time stamp)를 의미한다. T_d 는 호스트에 의한 상기 S2-1 단계의 요청에 대해 약속된 시간 내에 A , E_{D_d} , E_{C_d} 가 호스트에게 도달되었는지 판단하기 위한 시간 길이로서, 그 시간 길이를 초과한 값(잘못된 값)이 온다면 외부로부터의 변조 또는 도청 등의 위협이 존재한다고 판단한다. 따라서 T_d 는 이러한 위협을 방지하기 위해 사용되는 것이다. 그리고 E_{D_d} 와 E_{C_d} 는 각각 DH 알고리즘에 의해 생성될 수 있다.
- [0029] 디바이스로부터 A , E_{D_d} , E_{C_d} 를 전송받은 호스트(2)는 KCK_h, PTK_h, MIC_h를 생성한다(S2-5). 이는 KCK_d, PTK_d, MIC_d를 생성하는 경우와 마찬가지로 생성할 수 있다. 호스트(2)는 $D_h [= h(A^b \bmod p)]$ 를 복호화 키로 하여 E_{D_d} 를 복호화하여 TKID와 T_d 를 추출하고, T_d 의 유효 여부를 검사하여(S2-6) 유효하다면 디바이스로부터 받은 TKID와 자신의 TKID가 일치하는지 검사한다(S2-7). T_d 의 유효 여부 판단 기준은 본 발명에 의한 상호 인증 과정을 구현시에 미리 결정되며, WUSB가 구축된 환경 등 제반 요소를 고려해 결정된다. 그리고 $C_h [= h(HNonce) (+) D_h]$ 를 복호화 키로 하여 E_{C_d} 를 복호화하여 MIC_d를 추출하여 자신이 생성한 MIC_h와 일치하는지 검사한다(S2-8).
- [0030] T_d 가 유효하지 아니하거나 S2-7 단계 또는 S2-8 단계의 검사 결과 어느 하나라도 일치하지 않는 것으로 판단되면 상호 인증 과정(4-way handshake)은 더 이상 진행되지 아니하며, T_d 가 유효하고 S2-7 단계와 S2-8 단계의 검사 결과 모두 일치하는 것으로 판단되면 호스트(2)는 E_{D_d} , E_{C_d} 를 전송한 디바이스가 통신 채널을 설정할 수 있는 정당한 자격이 있는 것으로 예비적으로 판단하게 된다. 아울러 호스트는 S2-5 단계에서 생성되었던 PTK_h

를 디바이스와의 통신 세션에 이용될 후보 세션 키로 지정하게 된다(S2-9).

[0031] 다음으로 상호 인증 과정(4-way handshake)의 세 번째 단계(S3)로, 본 단계는 $E_{D,d}$, $E_{C,d}$ 를 전송한 디바이스가 상대방 호스트(2)가 자신과의 통신 채널을 설정할 수 있는 정당한 상대방인지 확인하는 단계이다. 본 단계(S3)는 아래와 같이 S3-1 내지 S3-4 단계로 구현된다.

[0032] 호스트(2)는 D_h 를 암호화 키로 암호화된 메시지 $E_{D,h}[\text{TKID} || \text{HNonce} || \text{MIC}_h || (T_d+1)]_{D,h}$ 를 생성하여 디바이스에게 전송한다(S3-1). $E_{D,h}$ 도 DH 알고리즘에 의해 생성될 수 있다.

[0033] $E_{D,h}$ 를 전송받은 디바이스는 $E_{D,h}$ 가 유효한지 판단하는데(S3-2), 이는 결국 $E_{D,h}$ 를 전송받은 디바이스가 이를 복호화하여 TKID, HNonce, MIC_h , T_d+1 을 추출한 후 TKID와 HNonce, T_d+1 의 유효 여부를 검사하는 것이다. $E_{D,h}$ 의 유효 여부 판단의 기준은 본 발명에 의한 상호 인증 과정을 구현시에 미리 결정되며, WUSB가 구축된 환경 등 제반 요소를 고려해 결정된다.

[0034] $E_{D,h}$ 가 유효하다면 디바이스는 S1-3 단계에서 생성했던 MIC_d 가 호스트(2)로부터 전송받은 MIC_h 와 일치하는지 검사한다(S3-3). $E_{D,h}$ 가 유효하지 아니하거나 MIC_d 가 MIC_h 와 일치하지 않는다면 디바이스는 더 이상 상호 인증 과정(4-way handshake)을 진행하지 않고 상호 인증 과정을 더 이상 진행하지 아니한다는 사실을 호스트(2)에 통지한다. 이러한 통지를 받은 호스트(2)는 자신이 생성했었던(후보 세션 키로 지정한) PTK_h 를 폐기시킨다. 하지만 $E_{D,h}$ 가 유효하고 MIC_d 가 MIC_h 와 일치한다면, 디바이스는 $E_{D,h}$ 를 보낸 호스트가 정당한 상대방임을 확인하게 되고, S1-3 단계에서 생성했던 PTK_d 를 호스트(2)와의 통신 세션에 이용될 자신의 세션 키로 확정하게 된다(S3-4).

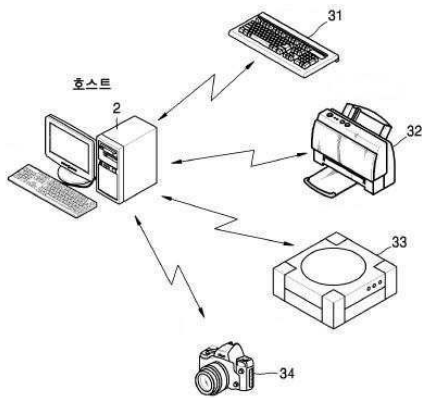
[0035] 다음으로 상호 인증 과정(4-way handshake)의 마지막 단계(S4)로, 디바이스가 호스트(2)에게 자신의 세션 키 PTK_d 를 성공적으로 구축하였음을 알린다. 호스트(2)는 S2-9 단계에서 후보 세션 키로 지정한 PTK_h 를 디바이스와의 통신 세션에 이용될 자신의 세션 키로서 최종 확정하게 된다. 이로써 호스트(2)와 디바이스는 서로 간에 안전한(신뢰된) 통신 채널을 구축하여 통신 세션을 개시하게 되며, 이후 디바이스와 호스트는 서로에게 안심하고 원하는 정보를 송수신할 수 있게 된다.

[0036] 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

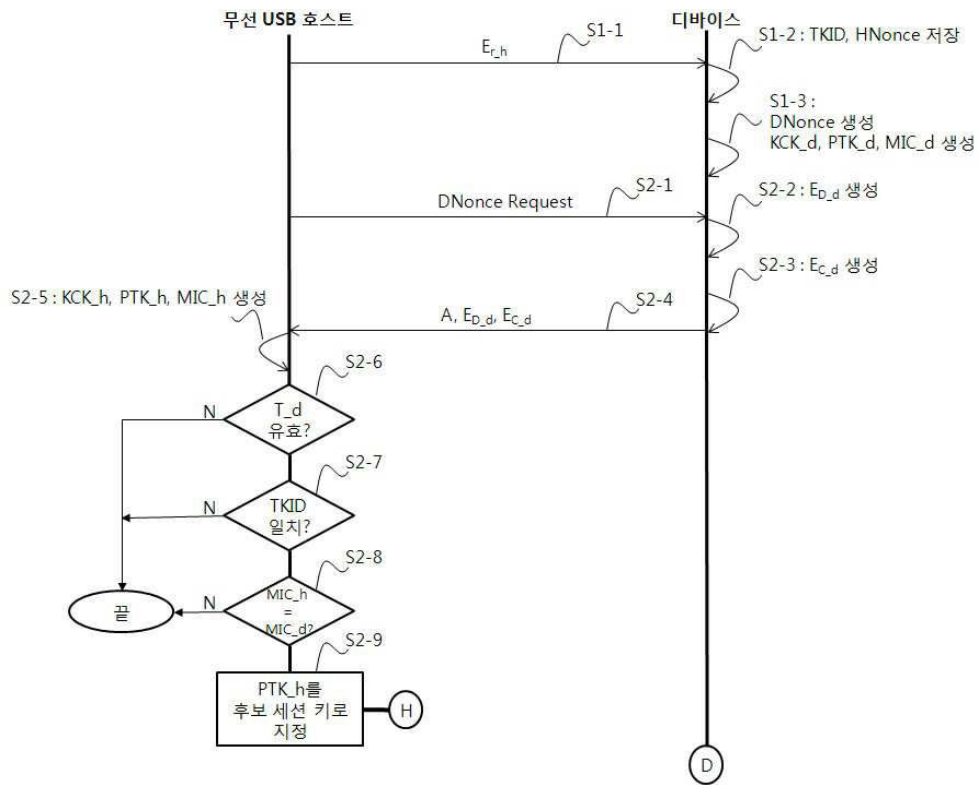
[0037] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예는 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

도면1



도면2a



도면2b

