(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/22 (2006.01)

(45) 공고일자 2006년12월01일
(11) 등록번호 10-0652017
(24) 등록일자 2006년11월23일

(21) 출원번호 10-2005-0119589
(22) 출원일자 2005년12월08일
심사청구일자 2005년12월08일

(65) 공개번호
(43) 공개일자

(73) 특허권자 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 구한승
대전 서구 만년동 초원아파트 101-809

정준영
대전 서구 만년동 상아아파트 109-207

권은정
대전 서구 만년동 초원아파트 101-1405

권오형
대전 유성구 어은동 한빛아파트 107-1103

이수인
대전 서구 둔산동 크로바아파트 106-606

(74) 대리인 특허법인 신성

심사관 : 김병균

전체 청구항 수 : 총 5 항

(54) 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법

(57) 요약

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은 닥시스(DOCSIS: Data Over Cable Service Interface Specification) 케이블 모뎀에 대한 해커의 물리적인 공격에 대해 FIPS PUB 140-2에서 규정한 물리적 보안 레벨을 올리지 않고도 보안이 요구되는 주요 데이터를 효과적으로 보호할 수 있게 하는, 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법을 제공하는데 그 목적이 있음.

3. 발명의 해결방법의 요지

본 발명은, 닥시스(DOCSIS) 규격을 따르는 케이블 모뎀(CM)의 물리적 보안 공격에 대한 보안 방법에 있어서, 상기 닥시스 케이블 모뎀에 저장될 정보(저장대상 정보)를 기밀성 요구 정도 및 변조금지 요구 정도에 따라 분류하는 정보 분류 단계; 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 기밀 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성(non-volatile) 메모리에 저장하되, 해커의 공격이 감지되면 상기 비휘발성 메모리 내에 저장된 정보를 삭제하는 메커니즘을 수행하는 기밀정보 보안 단계; 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '중간레벨 보안정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 중간레벨보안정보 보안 단계; 및 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 변조금지 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 WO 메모리(write-once 메모리)에 저장하는 변조금지정보 보안 단계를 포함함.

4. 발명의 중요한 용도

본 발명은 닥시스 케이블 모뎀의 보안 등에 이용됨.

대표도

도 1

특허청구의 범위

청구항 1.

닥시스(DOCSIS: Data Over Cable Service Interface Specification) 규격을 따르는 케이블 모뎀(CM)의 물리적 보안 공격에 대한 보안 방법에 있어서,

상기 닥시스 케이블 모뎀에 저장될 정보(저장대상 정보)를 기밀성 요구 정도 및 변조금지 요구 정도에 따라 분류하는 정보 분류 단계;

상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 기밀 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성(non-volatile) 메모리에 저장하되, 해커의 공격이 감지되면 상기 비휘발성 메모리 내에 저장된 정보를 삭제하는 메커니즘을 수행하는 기밀정보 보안 단계;

상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '중간레벨 보안정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 중간레벨보안정보 보안 단계; 및

상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 변조금지 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 WO 메모리(write-once 메모리)에 저장하는 변조금지정보 보안 단계

를 포함하는 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법.

청구항 2.

닥시스(DOCSIS) 규격을 따르는 케이블 모뎀(CM)의 물리적 보안 공격에 대한 보안 방법에 있어서,

상기 닥시스 케이블 모뎀에 저장될 정보(저장대상 정보)를 기밀성 요구 정도 및 변조금지 요구 정도에 따라 분류하는 정보 분류 단계;

상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 기밀 정보'이면, 상기 저장대상 정보를 암호화(key encapsulation)하여 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 기밀정보 보안 단계;

상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '중간레벨 보안정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 중간레벨보안정보 보안 단계; 및

상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 변조금지 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 WO 메모리(write-once 메모리)에 저장하는 변조금지정보 보안 단계

를 포함하는 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법.

청구항 3.

제 1 항 또는 제 2 항에 있어서,

상기 닥시스케이블 모뎀의 전원이 켜(ON)질 때마다, 상기 WO 메모리에 저장된 '절대 변조금지 정보'의 무결성을 검사하는 무결성 검사 단계

를 더 포함하는 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법.

청구항 4.

제 3 항에 있어서,

상기 무결성 검사 단계는,

상기 닥시스 케이블 모뎀의 전원이 켜질 때마다 FIPS PUB 140-2 "4.9.1. Power-up Test"에서 규정한 대로 '절대 변조금지 정보'의 변경 여부를 검사하는 것을 특징으로 하는 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법.

청구항 5.

제 4 항에 있어서,

상기 '절대 기밀 정보'는,

'닥시스 케이블 모뎀의 RSA 개인키/공개키 쌍', '케이블 랩스/제조사의 RSA 공개키', 중요보안파라미터(CSP)를 포함하고;

상기 '중간레벨 보안정보'는,

케이블 랩스/제조사의 인증서를 포함하며;

상기 '절대 변조금지 정보'는,

닥스케이블 모뎀의 인증서 및 부트로더(boot loader)를 포함하는 것을 특징으로 하는 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 국제 표준인 닥시스(DOCSIS: Data Over Cable Service Interface Specification) 규격을 따르는 케이블 모뎀의 물리적 보안 공격에 대한 보안 방법에 관한 것으로, 더욱 상세하게는 닥시스 케이블 모뎀에 대한 해커의 물리적인 공격에 대해 FIPS PUB 140-2(Federal Information Processing Standards Publication 140-2)에서 규정한 물리적 보안 레벨을 올리지 않고도 보안이 요구되는 주요 데이터를 효과적으로 보호할 수 있게 하는, 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법에 관한 것이다.

국제 표준인 닥시스(DOCSIS) 규격에서 제시하는 기본적인 물리적 보안 수준은 FIPS PUB 140-2에서 규정한 보안등급 중 제일 낮은 등급인 레벨 1 이다.

그리고, 닥시스(DOCSIS) 규격에서는, 닥시스 케이블 모뎀의 RSA 개인키/공개키 쌍(CM's RSA Key Pair) 및 케이블 모뎀의 인증서(CM's Certificate)는 물리보안공격으로부터 보호하기 위해 WO메모리(write-once Memory)에 저장하도록 규정하고 있다. 그 외 보안이 요구되는 케이블랩스(CableLabs) 또는 제조사의 인증서(CableLabs' or Manufacturer's Certificate), 케이블랩스(CableLabs) 또는 제조사의 RSA 공개키(CableLabs's or Manufacturer's RSA Public Key) 등은 일반적인 비휘발성 메모리에 저장하도록 규정하고 있다.

하지만, 닥시스 케이블 모뎀의 부트로더(boot-loader) 데이터는 절대 변경되어서는 안 되는 것임에도 불구하고, 이에 대한 물리적 공격의 대응 방법이 규격에 전혀 명시되어 있지 않다.

위에서 살펴본 바와 같이 닥시스 규격에서 규정하고 있는 케이블 모뎀의 물리적 보안 수준은 기본적으로 FIPS PUB 140-2에서 규정한 레벨 1을 제시하고 있으며 주요 보안이 요구되는 데이터들에 대해 특정 메모리에 저장하는 것만을 규정하고 있을 뿐이다.

이러한 닥시스 규격에서의 규정만으로는 전문적인 해커의 물리적인 공격으로부터 주요 데이터들이 매우 쉽게 노출 및 변경될 가능성이 매우 높다는 문제점이 있다. 왜냐하면 FIPS PUB 140-2에서 규정한 레벨 1에서는 물리적 보안을 위해 장치의 코팅 또는 봉인하는 정도의 보안 수준을 가지기 때문이다.

이에 대한 종래의 해결책으로는, FIPS PUB 140-2에서 규정한 물리적 보안 레벨을 3이상으로 올리는 방법이 있다. 하지만, 이 방법은 보안레벨을 올림으로써 케이블 모뎀의 단가가 올라가고 이는 사업 운용 비용의 증가를 초래하기 때문, 케이블 통신 사업자가 원하지 않는다는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기 문제점을 해결하기 위하여 제안된 것으로, 닥시스 케이블 모뎀에 대한 해커의 물리적인 공격에 대해 FIPS PUB 140-2에서 규정한 물리적 보안 레벨을 올리지 않고도 보안이 요구되는 주요 데이터를 효과적으로 보호할 수 있게 하는, 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법을 제공하는데 그 목적이 있다.

본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허청구범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

발명의 구성

상기 목적을 달성하기 위한 본 발명은, 닥시스(DOCSIS) 규격을 따르는 케이블 모뎀(CM)의 물리적 보안 공격에 대한 보안 방법에 있어서, 상기 닥시스 케이블 모뎀에 저장될 정보(저장대상 정보)를 기밀성 요구 정도 및 변조금지 요구 정도에 따라 분류하는 정보 분류 단계; 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 기밀 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성(non-volatile) 메모리에 저장하되, 해커의 공격이 감지되면 상기 비휘발성 메모리 내에 저장된 정보를 삭제하는 메커니즘을 수행하는 기밀정보 보안 단계; 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '중간레벨 보안정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 중간레벨보안정보 보안 단계; 및 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 변조금지 정보'이면,

상기 저장대상 정보를 상기 닥스 케이블 모뎀의 WO 메모리(write-once 메모리)에 저장하는 변조금지정보 보안 단계를 포함한다. 또한, 상기 본 발명은, 상기 닥시스케이블 모뎀의 전원이 켜(ON)질 때마다, 상기 WO 메모리에 저장된 '절대 변조금지 정보'의 무결성을 검사하는 무결성 검사 단계를 더 포함한다.

한편, 본 발명은, 닥시스(DOCSIS) 규격을 따르는 케이블 모뎀(CM)의 물리적 보안 공격에 대한 보안 방법에 있어서, 상기 닥시스 케이블 모뎀에 저장될 정보(저장대상 정보)를 기밀성 요구 정도 및 변조금지 요구 정도에 따라 분류하는 정보 분류 단계; 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 기밀 정보'이면, 상기 저장대상 정보를 암호화(key encapsulation)하여 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 기밀정보 보안 단계; 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '중간레벨 보안정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 비휘발성 메모리에 저장하는 중간레벨보안정보 보안 단계; 및 상기 정보 분류 단계에서의 분류 결과, 상기 저장대상 정보가 '절대 변조금지 정보'이면, 상기 저장대상 정보를 상기 닥스 케이블 모뎀의 WO 메모리(write-once 메모리)에 저장하는 변조금지정보 보안 단계를 포함한다. 또한, 상기 본 발명은, 상기 닥시스케이블 모뎀의 전원이 켜(ON)질 때마다, 상기 WO 메모리에 저장된 '절대 변조금지 정보'의 무결성을 검사하는 무결성 검사 단계를 더 포함한다.

본 발명은, 메모리에 중요 데이터를 저장할 때 해커의 공격이 예상될 때 메모리 내 정보를 삭제하는(key zeroization) 메커니즘 사용하거나 또는 데이터를 암호화(key encapsulation)하여 저장하는 방법으로 물리적 공격을 차단한다. 또한 케이블 모뎀의 전원이 켜질 때마다 FIPS PUB 140-2에 규정된 "Power-up Test"로 부트로더 데이터의 무결성을 체크한다.

상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명하기로 한다.

도 1은 본 발명에 따른 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법에 대한 일실시예 흐름도로서, 닥시스 케이블 모뎀 보안 정보 저장 정책을 나타낸다.

본 발명은 닥시스 케이블 모뎀 제조사는 모뎀 제조시 닥시스 BPI+ (Baseline Privacy Interface) 규격에 따라 닥시스 케이블 모뎀(CM)의 RSA 개인키/공개키 쌍(CM's RSA Key Pair)(101), 케이블랩스(CableLabs) 또는 제조사의 RSA 공개키(CableLabs's or Manufacturer's RSA Public Key)(101), 중요보안파라미터(CSP: Critical Security Parameter)(101), 케이블랩스(CableLabs) 또는 제조사의 인증서(CableLabs' or Manufacturer's Certificate)(105), 그리고 닥시스 케이블 모뎀의 인증서 및 닥시스 케이블 모뎀의 부트로더(boot-loader)(CM's Certificate and CM's boot-loader)(107)들을 해커의 물리보안공격(Physical Security Attack)으로부터 보호하기 위해, 어떻게 닥시스 케이블 모뎀 내의 메모리에 저장해야 하는지 그리고 어떤 종류의 메모리에 저장해야 하는지를 규정한다.

즉, 본 발명은, 저장 대상이 되는 정보의 유형에 따라, 저장되는 메모리나 그 저장 방식을 달리하는 것을 특징으로 한다. 저장 대상이 되는 정보는 기밀성 요구 정도 및 변조금지 요구 정도에 따라, 절대적으로 기밀성 보장이 요구되는 '절대 기밀 정보', 절대적으로 변조가 금지되어야 하는 '절대 변조금지 정보', 및 그 외의 '중간레벨 보안정보'로 분류된다.

먼저, 저장될 정보가 '절대 기밀 정보', 즉 닥시스 케이블 모뎀의 RSA 개인키/공개키 쌍(CM's RSA Key Pair)(101), 케이블랩스(CableLabs) 또는 제조사의 RSA 공개키(CableLabs's or Manufacturer's RSA Public Key)(101), 중요보안파라미터(CSP: Critical Security Parameter)(101)인 경우에는, 닥시스 케이블 모뎀 제조사가 이들 정보를 암호화된 형태로 저장하길 원하는지, 아니면 평문 형태로 저장되길 원하는 지에 따라 다음의 두 가지 방법을 선택적으로 사용하여 저장한다(102).

만약, 닥시스 케이블 모뎀 제조사가 상기 "101"의 정보를 평문 형태로 메모리에 저장하고자 하는 경우라면, 비휘발성(non-volatile) 메모리에 저장하되, 해커의 공격이 예상되면 메모리 내 정보를 삭제하는(key zeroization) 메커니즘을 수행한다(103).

이와 반대로, 닥시스 케이블모뎀 제조사가 상기 "101"의 정보를 암호화된 형태로 저장하고자 하는 경우라면, 상기 "101"의 정보를 암호화하여(key encapsulation)(104), 비휘발성(non-volatile) 메모리에 저장한다(106).

두번째, 저장될 정보가 '중간레벨 보안정보', 즉 케이블랩스(CableLabs) 또는 제조사의 인증서(CableLabs' or Manufacturer's Certificate)(105)인 경우에는 반드시 케이블 모뎀의 비휘발성(non-volatile)메모리에 저장해야 한다(106).

마지막으로, 저장될 정보가 '절대 변조금지 정보', 즉 닥시스 케이블 모뎀의 인증서(CM's Certificate), 및 닥시스 케이블 모뎀의 부트로더(boot-loader)(CM's boot-loader)인 경우에는 반드시 케이블 모뎀의 WO 메모리(write-once 메모리)에 저장해야 한다(108).

도 2는 본 발명에 따른 닥시스 케이블 모뎀 부트로더(boot-loader) 변경여부 검사 방법에 일실시예 흐름도이다.

닥시스 케이블 모뎀의 부트로더(boot-loader)는 어떠한 경우에서도 변경 가능해서는 안 된다.

이를 확인하기 위해 닥시스 케이블 모뎀의 전원이 켜질 때(Power-Up)마다(201), FIPS PUB 140-2 "4.9.1. Power-up Test"에서 규정한 대로 부트로더(boot-loader) 데이터의 변경 여부(무결성)를 검사한다(202).

상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

발명의 효과

상기와 같은 본 발명은, 닥시스 케이블모뎀 제조사가 FIPS PUB 140-2에서 규정한 보안등급 중 제일 낮은 등급인 레벨1을 만족하면서도 효과적으로 해커에 의한 닥시스 케이블모뎀 물리보안공격에 대하여 대응할 수 있게 하는 효과가 있다.

또한, 본 발명에 따르면, 닥시스 케이블 모뎀 제조사는 해커에 의한 물리보안공격을 막기 위해 FIPS PUB 140-2의 높은 보안등급을 채택하지 않아도 되기 때문에, 제조 비용을 줄일 수 있게 하는 효과가 있다.

또한, 본 발명은, FIPS PUB 140-2 4.9.1. Power-up Test에서 규정한 방식에 따라 닥시스 케이블 모뎀 부트로더(boot-loader)의 변경 여부를 닥시스 케이블 모뎀의 전원이 켜질 때마다 검사하기 했기 때문에, 부트로더(boot-loader)의 무결성(integrity)을 용이하게 확인할 수 있게 하는 효과가 있다.

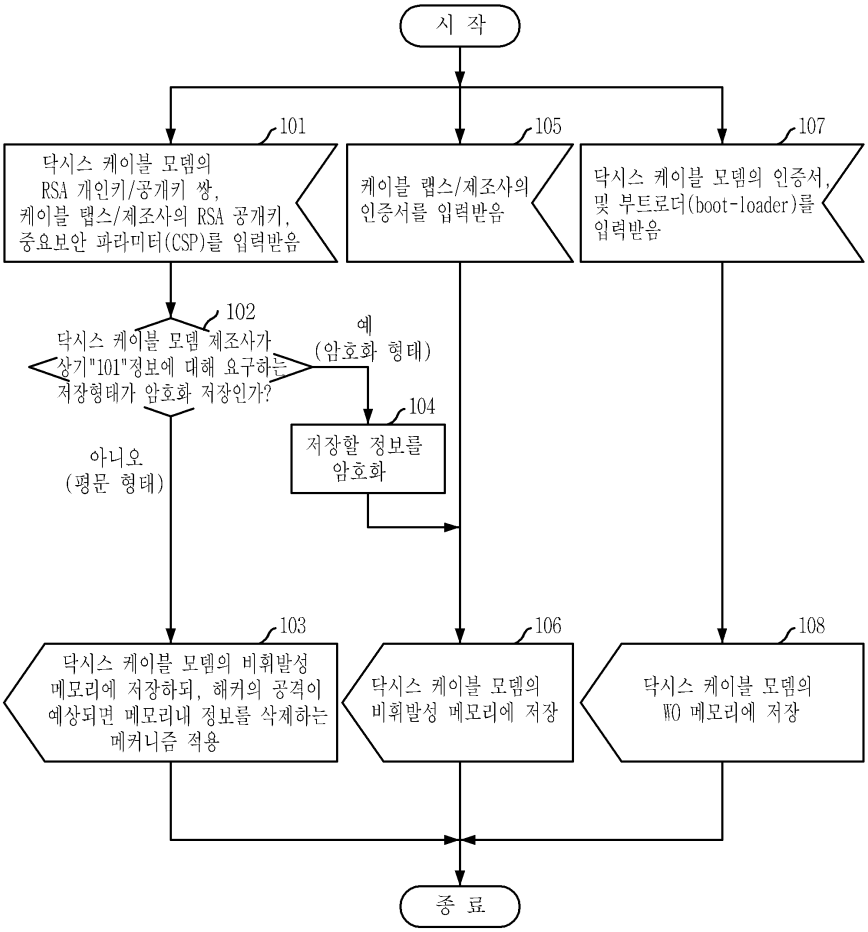
도면의 간단한 설명

도 1은 본 발명에 따른 물리보안공격에 대한 닥시스 케이블 모뎀의 보안 방법에 대한 일실시예 흐름도,

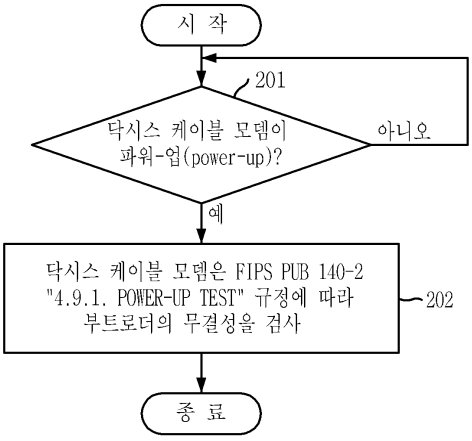
도 2는 본 발명에 따른 닥시스 케이블 모뎀 부트로더(boot-loader) 변경여부 검사 방법에 일실시예 흐름도이다.

도면

도면1


시 작
101
닥시스 케이블 모뎀의
RSA 개인키/공개키 쌍,
케이블 랩스/제조사의 RSA 공개키,
중요보안 파라미터(CSP)를 입력받음
105
케이블 랩스/제조사의
인증서를 입력받음
107
닥시스 케이블 모뎀의 인증서,
및 부트로더(boot-loader)를
입력받음
102
닥시스 케이블 모뎀 제조사가
상기"101"정보에 대해 요구하는
저장형태가 암호화 저장인가?
예
(암호화 형태)
104
저장할 정보를
암호화
아니오
(평문 형태)
103
닥시스 케이블 모뎀의 비휘발성
메모리에 저장하되, 해커의 공격이
예상되면 메모리내 정보를 삭제하는
메커니즘 적용
106
닥시스 케이블 모뎀의
비휘발성 메모리에 저장
108
닥시스 케이블 모뎀의
I/O 메모리에 저장
종 료

도면2


시 작
201
닥시스 케이블 모뎀이
파워-업(power-up)?
아니오
예
닥시스 케이블 모뎀은 FIPS PUB 140-2
"4.9.1. POWER-UP TEST" 규정에 따라
부트로더의 무결성을 검사
202
종 료