안전한 전자봉인을 위한 인증 프로토콜 설계

박성수[O1] 이문규[1)2] 김동규[2)3] 박근수[1] 김호원[4] 정교일[4]
[1]서울대학교 컴퓨터 공학부, [2]인하대학교 컴퓨터 공학부,
[3]부산대학교 컴퓨터공학과, [4]한국전자통신연구원
[1]{sspark[O], kpark}@thoery.snu.ac.kr, [2]mklee@inha.ac.kr, [3]dkkim@islab.ce.pusan.ac.kr, [4]{khw, kyoil}@etri.re.kr

Design of an authentication protocol for secure electronic seals

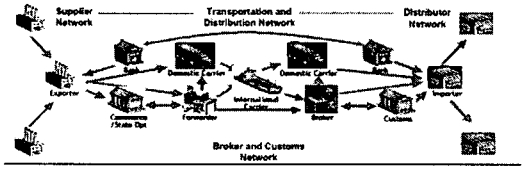
Seongsoo Park[01] Mun-Kyu Lee[2] Dong Kyue Kim[3] Kunsoo Park[1] Howon Kim[4] Kyoil Chung[4]
[1]Seoul National University, [2]Inha University, [3]Pusan National University,
[4]Electronics and Telecommunications Research Institute

요 약

최근 국제물류에서 화물 컨테이너의 운송을 보다 안전하고 효율적으로 관리하기 위하여 수출입절차 규제가 강화되고, 도난, 밀매, 테러 등의 범죄를 예방하기 위한 새로운 정책과 기술이 도입되고 있다. 특히, 빠르게 실용화가 진행되고 있는, RFID 기술을 사용한 무선인식 전자봉인(e-seal)은 기존의 기계적 봉인장치를 대체함으로써 컨테이너 운송의 안전성을 보장하고, 선적 및 하선 절차의 효율을 높인다. 수년간 e-seal의 ISO 국제표준화가 진행되어 왔으며, 최근 e-seal의 데이터 보호에 대한 표준화가 진행 중이다. 본 논문에서는 e-seal의 실질적인 사용 환경과 기존의 명령어 표준규격을 고려하여 안전한 e-seal을 위한 새로운 명령어들을 설계하고, EAP를 응용하여 e-seal과 리더기간의 상호 인증 프로토콜을 제시한다. 그리고 이를 다시 효율적으로 개선하여 e-seal에 적합한 상호 인증 프로토콜을 제시한다.

1. 서 론

최근 미국을 중심으로 국제 화물 컨테이너의 운송을 보다 안전하고 효율적으로 관리하기 위한 수출입절차 보안정책이 강화되고 있다. 이전에는 도난피해로 인한 손실이나 밀매적발이 국제물류안전의 최대 관심사였지만, 미국의 9.11테러 이후, 국제유통 네트워크를 통한 테러위협 방지에 세계적인 관심이 높아졌다. 컨테이너 운송은 단계별로 다양한 사업자 및 관계 당국들이 관련되어 (그림 1)[1]과 같이 복잡한 운송 네트워크를 가지며, 각 노드와 운송에 대한 안전 정책이 마련되어야 한다.



(그림 1) Supply Chain Security

화물 컨테이너 운송의 안전은 컨테이너 무결성, 접근제어, 위치추적, 위험화물 선별 등의 여러 측면에서 고려되어야 하고, 동시에 안전과 능률의 측면에서 균형 있는 개선 방향을 모색해야한다. 이를 위하여, 컨테이너 운송의 효율적인 안전 관리를 위한 새로운 정책과 기술이 도입되고 있다. 특히, 미국을 중심으로 스마트 컨테이너(Smart Container)[2]의 개념이 수년 안에 실용화될 전망이며, 현재는 active RFID 태그장치를 사용한 무선인식 전자봉인(e-seal)의 사용이 의무화되고 있는 추세이다.

본 논문에서는 e-seal의 현 표준 규격이 가지는 데이터 보안상의 취약점을 보완한 안전한 e-seal 명령어를 제시하고 리더기와의 효율적인 상호 인증 프로토콜을 제시한다.

1) 본 연구는 한국전자통신연구원 "RFID 프라이버시 프로토콜 검증 기술 연구" 과제의 지원에 의하여 수행되었음
2) 이 논문은 교육인적자원부 지방연구중심대학육성사업 (차세대물류IT기술연구사업단)의 지원에 의하여 연구되었음

2. 기본 지식

2.1. 봉인장치(Seal)

컨테이너에 화물을 적재하고 문에 붙이는 봉인장치로서, 운송과정에서의 컨테이너 무결성을 보장하는, 즉, 적재한대로 도착되었음을 확인하는 안전장치이다. 최근까지는 기계적 봉인장치가 주로 사용되고 있으며, 그에 관한 국제 표준 규격은 ISO/PAS 17712[3] 이다.

2.2. 전자봉인(e-seal)

E-seal은 RFID(Radio Frequency IDentification) 기술을 사용하여 원격에서 자동으로 봉인상태를 확인할 수 있는 컨테이너 봉인장치를 말한다.

e-seal의 일반적인 요구사항은 다음과 같다.[1][4][5][6][7][8] (1) 유일한 seal ID를 가지며, (2) 최소 물리적 특성에 관한 ISO/PAS 17712 규격을 만족해야한다. (3) 봉인(seal), 개봉(unseal) 등의 동작 event, (4) 위치추적(checkpoint, GPS) 정보, (5) 온도, 진동 등을 감지하는 센서 정보를 날짜/시간과 함께 로그로 저장하고, (6) 위험요소가 감지되면 즉각 경고 메시지를 전송한다. 그 외에, 위성통신을 통한 실시간 위치추적 기능, 컨테이너 내부 화물의 변화 인식, 사용자 정보의 읽기/쓰기, 재사용성 등의 부가적인 요구사항이 있을 수 있다.

이를 위하여, seal, 위치추적, 센서 기능을 통합한 e-seal은 다음과 같은 이점을 제공한다.[1][2][4] 경제적인 면에서 (1) 운송 화물의 탈선 및 지연 도착에 대한 신속한 대비책을 마련할 수 있고, (2) 창고 및 항만 터미널의 효율적인 운영과, (3) 도난 손실을 줄임으로써 물류비용을 절감할 수 있다. (4) 안전 관리의 자동화를 제공하여 사람들의 부주의와 실수로 인한 안전피해를 줄일 수 있다. 보안적인 면에서 (5) 컨테이너의 운송 경로, 화물 정보 등을 통하여 효율적으로 위험 컨테이너를 선별함으로써 밀매, 테러 등의 방지에 도움을 준다.

2.3. E-seal 국제 표준 동향

ISO TC104 SC4 WG2에서 만든 e-seal 표준문서는 ISO 18185-1[5], 2[6], 3[7], 7[8]이 있다. 이 중에서 18185-2, 3은 투

표가 진행 중이다. 하지만, Motorola의 보고서[9]에서 (1) 현 규격을 실제 항만환경에서 적용할 경우 전송지연으로 인한 저조한 인식률 문제, (2) e-seal의 데이터 보안상의 취약점과 현 규격에서 이를 해결하기 위해서는 전송시간이 더욱 연장된다는 문제, (3) 다른 기기와의 공동 운용이 어렵다는 문제가 제기되었다. 현재 (1)번 문제점이 해결될 때까지 18185-1, 7은 보류된 상태이며, (2)번 문제점과 관련하여 e-seal의 Data Protection에 관한 표준문서 18185-4가 다시 진행되고 있다.

3. E-seal의 데이터 보호를 위한 운용 정책

안전한 e-seal의 운용 정책에 대하여 다음과 같이 가정한다.

(1) 기존 ISO 18185 표준 규격을 그대로 따른다.

(2) e-seal은 운송 중에 발생하는 정보만을 로그에 저장한다. 예를 들어, e-seal 동작 event, 주기적인 위치추적, 센서감지, seal status 정보 등을 기록한다.

(3) 운송 중 변하지 않는, 수출입 관련 정보는 수출입물류를 관리하는 중앙서버에 seal ID와 함께 저장되고, 리더기는 seal ID를 통하여 중앙서버로부터 수출/수입업자, 운송회사, 출발/도착항, 컨테이너 ID 등을 확인한다.

(4) 인증 및 암호화를 위하여 표준 대칭키 암호 알고리즘 AES를 사용한다. 공개키 알고리즘은 계산 비용이 너무 크기 때문에 e-seal에 부적합하다.

(5) e-seal 인증에 필요한 공유키 정보는 e-seal의 제조자가 seal ID와 함께 물리적으로 세팅하여, 사용자에게 e-seal과 함께 판매한다.

(6) e-seal의 인증 정보는 리더기와 연결된 중앙서버에만 있다. 리더기는 중앙서버의 인증을 받고, e-seal의 인증 정보를 받는다. e-seal은 중앙서버가 인증한 리더기를 통하여 중앙서버를 인증한다.

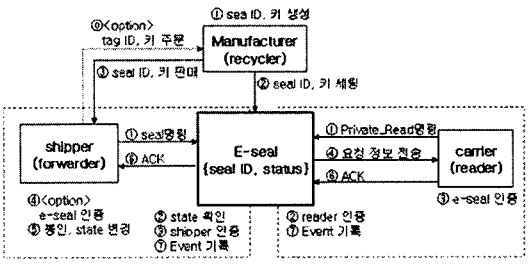
4. 안전한 e-seal 명령어 설계

안전한 e-seal을 위하여, 18185 표준의 명령어 형식에 따라, 추가한 명령어는 (표 1)과 같다. e-seal의 봉인(개봉)을 사용자의 인증 후에 동작하도록 하고[10], e-seal의 비밀 데이터를 사용자 인증 후에 읽고 쓰도록 하는 명령이 필요하다. 추가적으로 e-seal을 봉인하기 전에 위험상황 등의 동작 환경 설정을 사용자가 세팅하는 Initialize명령과, 기존 규격에 있는 alarm 기능에서, 리더기가 e-seal 인증 후 적법한 경고만을 처리하도록 새로운 Alert명령이 필요하다. 각 명령에 대하여, 운용 상황을 고려하여 상호 또는 단방향 인증 명령으로 분류하였다.

Code	Name	Type	인증	설 명
0x70	Seal	P2P	단방향	봉인권한을 가진 사용자가 e-seal에게 봉인 명령
0x72	Unseal	P2P	상호	봉인해제권한을 가진 사용자가 e-seal의 봉인해제 명령
0x74	public-Read	P2P	없음	임의의 리더기가 e-seal의 공개 정보 전송을 요청
0x76	private-Read	P2P	상호	특정 리더기가 e-seal에게 비공개 정보 전송을 요청
0x7C	Write	P2P	상호	특정 리더기가 e-seal에게 전송하는 운송정보 기록을 요청
0x7E	Alert	BC	단방향	e-seal이 위험상황을 리더기로 알리는 경고
0x7A	Initialize	P2P	단방향	봉인 전에 e-seal 동작 환경 설정

(표 1) 안전한 e-seal 명령어 세트

(그림 2)는 주요 명령에 대하여 사용자와 e-seal사이의 명령 수행 흐름을 나타낸 것이다. 이 때, 리더기와 e-seal의 인증 작업은 필수이지만, 컨테이너 터미널에서의 e-seal 인식성능 및 배터리 효율을 고려하여, 안전성과 효율성의 측면에서 e-seal에 적합하도록 인증 프로토콜의 메시지를 최소화하는 것이 중요하다.



(그림 2) 안전한 e-seal의 주요 명령 프로시져

5. E-seal 인증 프로토콜

5.1. 인증 프로토콜 설계

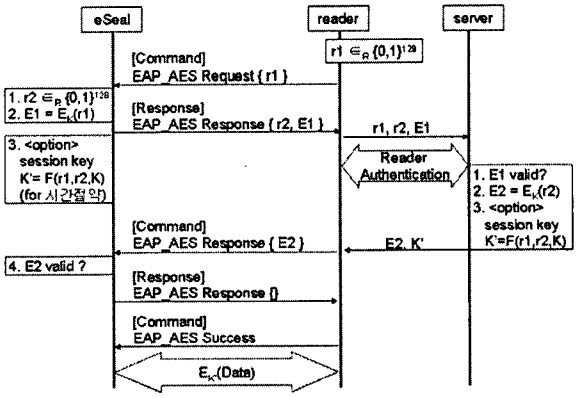
E-seal과 통신하는 리더기는 일반적으로 중앙서버와 연결되어 있으며, 이 중앙서버는 e-seal의 인증을 위한 공유키와 e-seal이 부착된 화물의 정보를 보관한다. 리더기는 중앙서버로부터 e-seal의 인증 결과를 확인하여 e-seal에게 전달한다.

이러한 구조는 무선랜 환경에서 사용자가 액세스포인트(AP)를 통하여 AAA 서버[11]와 인증을 하는 구조와 비슷하다. 실질적으로 다량의 e-seal을 인증해야하는 컨테이너 터미널과 같은 환경에서는 리더기와 인증 서버의 안정된 통신 채널이 보장된다고 가정할 수 있다. 무선랜 네트워크에서 가입자 인증에 사용되는 EAP[11]를 응용하면, AP에 해당하는 리더기의 인증은 중앙서버가 담당하므로, e-seal의 통신 부하가 줄어들고, 배터리 수명을 효과적으로 개선할 수 있다.

다만, 무선랜 환경에서는 AP가 프록시의 역할만을 수행하고 사용자와 AAA 서버가 데이터를 교환하는 반면, 리더기는 e-seal의 인증을 위한 프록시 역할을 한 후, e-seal과 데이터를 주고받은 주체이기 때문에, e-seal이 리더기의 identity를 인증하는 작업이 필요하다.

5.2. EAP 응용 e-seal 상호 인증 프로토콜

무선랜 네트워크에서 가입자 인증에 사용되는 EAP를 응용하여, 안전한 e-seal의 상호 인증 프로토콜을 (그림 3)과 같이 설계하였다.

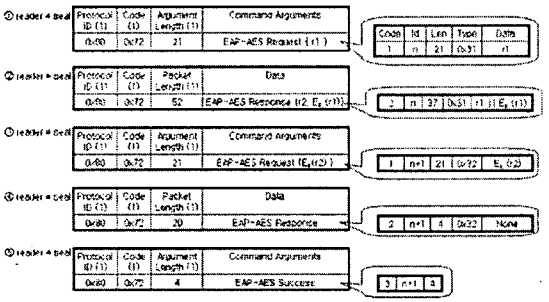


(그림 3) EAP 응용 상호 인증 프로토콜

제안된 프로토콜은 기본적인 대칭키 K를 사용하여 암호(AES)를 사용한 challenge-response 형식으로 상호 인증을 수행한다. (1) 먼저, 리더기가 e-seal에게 (상호 인증이 필요한) command를 보낸다. 이 때, 인자로 challenge r1이 포함된 EAP_AES Request 메시지가 전송된다. (2) e-seal은 자신의 인증을 위한 response $E_K(r1)$를 EAP_AES Response 메시지에 보내고, 동시에 서버 인증을 위한 challenge r2를 보낸다. (3) 리더기는 e-seal로부터 받은 메시지를 서버로 전달하면서,

e-seal 인증을 요청한다. (4) 이미 정의된 방식으로 서버는 리더기를 인증한 후, e-seal 인증 결과와, 서버 자신을 인증하기 위한 response $E_K(r2)$를 리더기로 전달한다. (5) 리더기는 e-seal에게 서버의 response를 전달하고, e-seal은 서버를 인증한다. 이를 통하여 리더기가 인증된 것임을 확인한다. (6) 프로토콜을 마치기 위해 e-seal은 EAP_AES Response를 보내고, 인증자인 리더기가 e-seal에게 EAP Success/Failure를 보냄으로써 인증과정이 종료된다. 인증 후에 리더기와 e-seal간의 데이터통신이 필요한 경우, 공유키(K)와 두 challenge r1, r2로 만들어진 session key K'을 사용하여 리더기와 e-seal간의 데이터 교환이 안전하게 이루어지도록 한다.

(그림 4)는 [5]와 [11]에서 정의된 메시지 형식에서 중요 필드만을 표시한 e-seal의 인증 메시지 형식을 나타낸 것이다.

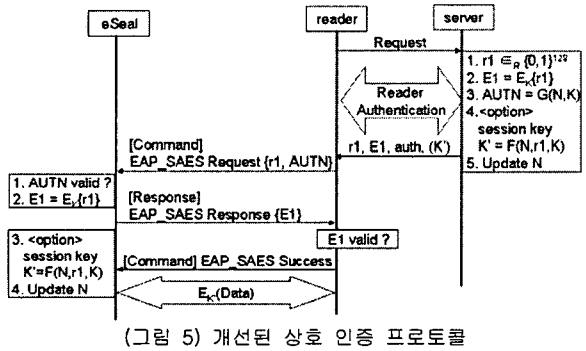


(그림 4) e-seal과 리더기사이의 인증 메시지 형식

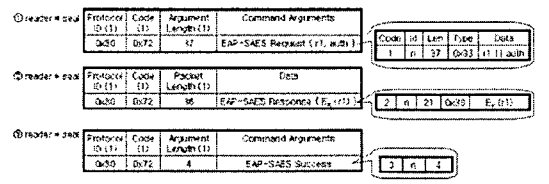
5.3. 개선된 상호 인증 프로토콜

5.2의 프로토콜에서는 e-seal과 서버가 각각 challenge를 생성하여 상호 인증한다. 그 대신, e-seal과 중앙서버가 공유하는 일종의 시퀀스 번호(N)를 사용하여 서버인증정보(AUTN)를 생성하는 방식을 사용하면, e-seal이 복잡한 challenge를 생성할 필요가 없어지고, 메시지의 수도 줄어들어, e-seal에 보다 적합하게 개선할 수 있다. (그림 5)는 (그림 3)의 프로토콜을 보다 효율적으로 개선한 상호 인증 프로토콜 나타내고 있다.

(그림 6)은 [5]와 [12]에서 정의된 메시지 형식에 맞추어 주요 필드만을 표시하여 e-seal이 송수신하는 인증 메시지 형식을 나타낸 것이다.



(그림 5) 개선된 상호 인증 프로토콜



(그림 6) 개선된 프로토콜을 위한 인증 메시지 형식

개선된 프로토콜은 다음과 같이 동작한다. (1) 리더기가 서버에게 먼저 e-seal의 인증 요청 메시지를 보내면, 중앙서버는 리더기를 인증한 후, e-seal과 공유하고 있는 N을 사용하여 서버 자신의 인증정보(AUTN)와 e-seal을 인증하기 위한 challenge r1을 리더기로 전달한다. 이 때, 리더기는 challenge r1에 대한 response와 session key K'도 전달받는다. (2) e-seal은 리더기를 통하여 전달받은 서버인증정보(AUTN)를 확인하여 서버를 인증하고, 이를 전달한 리더기도 인증되었음을 확인한다. (3) 마지막으로 리더기가 e-seal로부터 전달받은 response E1을 확인하여 e-seal에게 EAP Success/Failure를 보내면 인증과정이 종료된다. (4) 그리고 e-seal과 서버는 각각 내부적으로 같은 알고리즘을 수행하여 시퀀스 번호(N)를 갱신한다. 선택적으로, e-seal과 서버가 만든 session key K'를 사용하여 리더기와 안전하게 데이터를 교환한다.

5.4. 단방향 인증

e-seal의 운용 정책에 따라, 단반향 인증만이 필요한 경우에는 단방향 인증만하여 인증 메시지의 크기를 줄이는 것이 좋을 것이다. 단방향 인증 프로토콜은 5.2와 5.3에 제시된 상호 인증 프로토콜로부터 쉽게 설계할 수 있다.

6. 향후 연구 계획

위에서 e-seal의 데이터 보호를 위한 명령어들과 상호 인증 프로토콜을 설계하였다. 제안된 프로토콜은 상호 인증을 통한 접근 제어와 e-seal의 내부에서 키를 생성하여 리더기와 암호화 통신을 함으로써 데이터 기밀성을 보장할 수 있다. 하지만, 실질적인 공격 시나리오를 고려한 안전성 검증은 반드시 필요하다. 또한, e-seal 상호 인증 프로토콜의 효율성을 더욱 향상시키기 위한 방안에 대한 지속적이고 다각적인 연구가 계속되어야 한다. 현재 진행되는 e-seal의 국제 표준화에 국내에서도 적극적으로 참여할 것이며, 그 결과에 따라 설계한 프로토콜을 수정할 수 있다. 마지막으로, 안전한 e-seal을 위한 상호 인증 프로토콜을 구현하여 실질적으로 e-seal 제품에 적용하기 위하여 더욱 구체적인 검토가 진행될 예정이다.

7. 참고문헌

[1] Laurance Alvarado, BearingPoint, "Protecting the Supply Chain From Disasters", US-Mexico Trade Security Symposium, 2005.01.25

[2] World Shipping Council, International Mass Retail Association, National Industrial Transportation League, "In-Transit Container Security Enhancement", 2003.09.09

[3] ISO/PAS 17712, "Freight containers - Mechanical seals", 2003.10.01

[4] Adelina Balog, Junwei Jonathan Lim, Kendra Nettleton, "Riding the Wave on Ship Container Seal and Tracking System", 2003.06.03

[5] ISO/DIS 18185-1, "Freight containers - Electronic seals - Part 1:Communication protocol", 2005.04.28

[6] ISO 18185-2, "Freight containers - Electronic seals - Part 2:Application requirements", 2005.04.28

[7] ISO 18185-3, "Freight containers - Electronic seals - Part 3:Environmental characteristic", 2005.04.28

[8] ISO/DIS 18185-7, "Freight containers - Electronic seals - Part 7:Physical layer", 2005.04.28

[9] Motorola, Inc.,"Second report of detailed container use cases and deficiencies inthe ISO 18185-1, ISO 18185-7, and ISO 18000 standard", 2005.07.17

[10] Decker, C., Beigl, M, Krohn, A., Kubach, U., Robinson, P. "eSeal - A System for Enhanced Electronic Assertion of Authenticity and Integrity of Sealed Items". Pervasive 2004, Wien, Austria, LNCS, Vol. 3001, pp.254-268.

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, "Extensible Authentication Protocol(EAP)", IETF RFC 3748, 2004.06

[12] J. Arkko, H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", 2004.12.21