International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:10, 2007

Design of an Authentication Protocol for Secure Electronic Seals

Seongsoo Park, Mun-Kyu Lee, Dong Kyue Kim, Kunsoo Park,
Yousung Kang, Sokjoon Lee, Howon Kim, and Kyoil Chung

***Abstract*—**Electronic seal is an electronic device to check the authenticity and integrity of freight containers at the point of arrival. While RFID-based eSeals are gaining more acceptances and there are also some standardization processes for these devices, a recent research revealed that the current RFID-based eSeals are vulnerable to various attacks. In this paper, we provide a feasible solution to enhance the security of active RFID-based eSeals. Our approach is to use an authentication and key agreement protocol between eSeal and reader device, enabling data encryption and integrity check. Our protocol is based on the use of block cipher AES, which is reasonable since a block cipher can also be used for many other security purposes including data encryption and pseudo-random number generation. Our protocol is very simple, and it is applicable to low-end active RFID eSeals.

***Keywords*—**Authentication, Container Security, Electronic seal, RFID

I. Introduction

BEFORE the terrorist attacks of September 11, 2001, international trade was moving towards easier trade and more efficient transport. Since the attacks, however, governments and industry have given extensive consideration to the issue of protecting international commerce from terrorist threats. One of the maritime security issues that have been given particular attention is the security of containerized cargo shipments [1].

The complexity of the process for completing containerized shipments makes it more difficult to ensure the security, since even a typical single container could also carry cargo for several customers, thus multiplying the number of parties and documents involved. While it seems impossible to guarantee the perfect maritime security, the possible issue is how to increase port security to desired levels while minimizing the economic impacts associated with impeding the maritime trade system [2].

An effective way to obtain a sufficient level of security is ensuring the authenticity and the integrity of cargo from 'the point of origin' [2]. Ensuring the authenticity and the integrity means ensuring that the loaded container carries legitimate cargo made by legitimate parties, that the container was not tampered with while transported and also that the cargo information bound to the container is not fraudulent. The 'point of origin' approach is reasonable because inspecting cargo on the high seas is practically impossible and inspecting cargo upon its arrival at the destination port could be too late to prevent an unexpected attack.

Manual cargo seals [3] have been a common example of security equipment for containers. They can indicate whether or not the sealed entrance has been compromised and they can also provide physical protection like locks. However, they do not offer any information as to where, when, under what circumstances, or by whom the seal was broken. They do not provide immediate reporting of a tamper event, either.

Electronic Seals, eSeals for short, have been suggested as a good alternative to solve these problems. An eSeal is a device to transmit container information as it passes a reader device, and issues alerts and error conditions if the container has been tampered with or damaged. Electronics can improve the seal process in the following ways [4]:

1) One important enhancement is that a breach or tamper attempt can be detected as it happens and the time of occurrence can be recorded for later reporting. Also immediate reporting of those events is possible so that authorities may interrupt improper activity.
2) Physical protection function can be improved by attaching intrusion detection sensors married to traditional barrier seal components such as steel bolts and cables.
3) It is possible to assure a complete and accurate audit trail for seal status through a shipment's chain of custody by determining the integrity of seal and recording the time and place of each transaction. This function can become richer if it is used with global positioning system (GPS).
4) Other useful functions can be added easily. For example, an eSeal can store sensor data such as light, temperature, and humidity and can report immediately if the predefined requirements for the shipment condition are violated.

There are several kinds of eSeals including infrared seals and

This work was supported by the "Verification technology for RFID privacy protection protocols" project granted by Electronics and Telecommunications Research Institute and also supported by the Regional Research Centers Program (Research Center for Logistics Information Technology) granted by the Korean Ministry of Education & Human Resources Development.

S. Park and K. Park are with Seoul National University, Seoul 151-742, Korea (e-mail: {sspark, kpark}@theory.snu.ac.kr).

M.-K. Lee is with Inha University, Incheon 402-751, Korea (corresponding author, phone: +82-32-860-7456, e-mail: mklee@inha.ac.kr).

D. K. Kim is with Pusan National University, Busan 609-735, Korea (e-mail: dkkim@islab.ce.pusan.ac.kr).

Y. Kang, S. Lee, H. Kim and K. Chung are with Electronics and Telecommunications Research Institute, Daejeon 305-350, Korea ({youskang, junny, khw, kyoil}@etri.re.kr).

remote reporting seals supporting satellite or cellular communications. Most popular ones, however, are RFID (radio frequency identification)-based eSeals. There are already many commercial RFID eSeal products and standardization activities such as ISO 18185 drafts by ISO TC 104/SC 4 [5-9].

While the introduction of eSeal can provide freight containers with tamper resistance, there is another problem that should be addressed, i.e., the tamper resistance of eSeal itself. Note that there are many possible attacks against the authenticity and integrity of eSeal. For example, an attacker can erase the tamper event log inside an eSeal, plant a fake event to the log, generate a fake alarm to deceive the reader device, and so on. Unfortunately, however, the current specifications on RFID eSeals do not provide any robust solution to these problems.

In this paper, we consider a typical scenario for eSeal usage, and describe security requirements for eSeals. Then we present two protocols for mutual authentication and key agreement between an eSeal and a reader device. Our protocol is based on the use of block cipher AES [10]. This approach is reasonable, since a block cipher can also be used for many other purposes to secure the eSeal; it can be used directly to encrypt the contents of eSeal and it can also be used as a building block for one-way hash functions and pseudo-random number generators. Our protocol is very simple so that it is applicable to low-end active RFID eSeals.

II. Electronic Seal

A. Standardization Activities for eSeal

The draft standard ISO 18185, established by ISO TC104/ SC4/WG2, defines application requirements, environmental characteristics and various protocols for eSeals [5-9]. However, a recent report by Motorola indicated that major deficiencies in the current ISO 18185 draft standard will lead to delayed or missed reads, inadequate security, and a lack of interoperability [11].

Especially, there was an extensive vulnerability assessment for eSeals in early 2005, and spoofing and cloning were identified as potential data integrity threats to eSeal. Hence device authentication is believed to be the highest priority solution to mitigate those identified risks, and the sSeal standard-setting work (ISO 18185-4 [8]) is being expanded to meet that objective.

B. Definition and Requirements for eSeal

According to the first generation standards of ISO 18185 [5], an eSeal is defined as a *read-only*, *non-reusable* freight container seal conforming to the high security seal defined in *ISO PAS 17712* [3], which is a standard for mechanical seals, and conforming to ISO 18185 or revision thereof that electronically evidences tampering or intrusion through the container doors. Under the terms of the current version of ISO 18185, an eSeal is required to have;

1) a unique seal identifier including the identification of the manufacturer, which is permanently programmed into the seal during manufacturing and cannot be modified,
2) a seal status identification system,
3) a battery status indicator, and
4) immediate alarming function.

The communications between an eSeal and a reader device are done using a command-response protocol, i.e., the reader always initiate a session using a command, and then the eSeal responds to it with appropriate data. The only exception is the 'Alert' message, which is initiated by an eSeal.

On the other hand, the second generation standard of ISO 18185 to enhance the security has added the requirements for data protection of eSeals [8] so that an eSeal should have;

5) a read/write memory, which conflicts with the definition of the first generation eSeal,
6) a confidential information or user data, and
7) a device authentication functionality.

To enhance security and efficiency further, an eSeal may have some optional functions such as real-time location tracking using checkpoints or satellites, and integrated sensors to perceive the change of inner circumstances of a container.

III. Security Issues for Electronic Seal

A. Basic Security Requirements for eSeal

In order to protect the communication between an eSeal and a reader device, a security protocol should provide the following common security services;

1) Mutual Authentication and Access Control: An eSeal and a reader device should be able to authenticate each other. An eSeal will respond only to commands from authenticated readers, and a reader will accept only data from authenticated eSeals.
2) Data Confidentiality: The data exchanged between an eSeal and a reader device should be protected from a third party's eavesdropping.
3) Data Integrity: It should be verifiable whether the data received are exactly as sent by an authenticated entity.
4) Data-Origin Authentication: It should be verifiable whether the source of received data is as claimed.
5) Replay Protection: The commands and responses should be fresh to the specific session. The replay of any message should be detected.

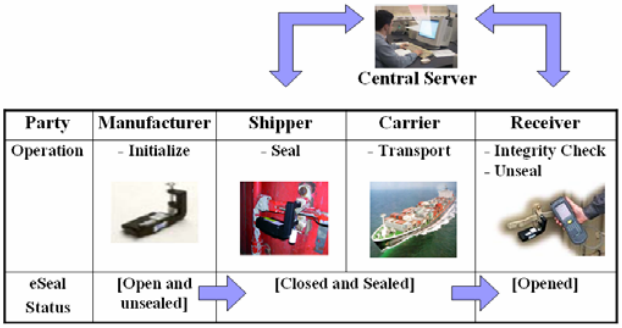

Fig. 1 Typical scenario for security-enabled eSeal usage

B. Operation Policy for Secure eSeal

Fig.1 shows a typical scenario by which a security-enabled eSeal is operated. Each of the steps is performed as follows;

1) When selling eSeals, the manufacturer provides the shipper with a set of cryptographic keys each of which is associated with each eSeal. This process should be done in a secure way, but we don't deal with this matter in this work. In this stage, the eSeal status is 'Open and unsealed.'
2) The shipper initializes the eSeal with the required information such as the manifest for shipment or the policy on the environment, e.g., a threshold temperature for valid transport. This 'write' operation should be controlled using cryptographic mechanisms to prevent an attacker's unauthorized write attempts. Our authentication protocol is used at this point.
3) After checking if required products are loaded completely and safely, the shipper seals the eSeal. Then the eSeal status becomes 'Closed and sealed.'
4) During the transportation, there would be several attempts to read the information in eSeal by carriers and checkpoints, or even by some attackers. While accesses to public information of an eSeal, e.g., seal ID, are always permitted, accesses to confidential information should be controlled by cryptographic mechanisms.
5) After the container arrives at the destination, the receiver can check the integrity of cargo by checking the status of the eSeal attached to the container. At this point, the eSeal should be authenticated, since it could have been spoofed or cloned while transported. The master key used by the receiver to authenticate the eSeal is assumed to have been transferred by the shipper via a central server.
6) If there is no problem, then the eSeal will be open by the receiver, and the eSeal status becomes 'Opened'.
7) Optionally the eSeal can be recycled after deleting the information on the previous shipment.

C. Assumption on the eSeal System

To deal with the above scenario and satisfy the above security requirements, we set the following assumptions;

1) AES-128 [10] is used as a cryptographic primitive for authentication and encryption. Note that the public-key primitives are not proper for eSeals due to its heavy computational costs.
2) A master key is permanently programmed into an eSeal during manufacturing process and is delivered to legitimate reader devices in a safe way, e.g., via a central server. This key is used for mutual authentication and derivation of session keys for integrity check and encryption.
3) There is a secure method to derive session keys from a master key. Although we don't deal with this problem in this paper, we mention that there are some effective methods such as pseudo-random functions using CBC-MAC [12].
4) There is a secure channel between a reader device and a central server. While we don't deal with this matter in this paper, we mention that we can use typical wired connection methods equipped with cryptographic mechanisms, such as SSL.

IV. Authentication Protocols

A. Basic Mutual Authentication Protocol

As we have mentioned in the previous section, we assume the existence of a backend server. It plays the role of authenticator of an eSeal, and a reader device consults this server about the cryptographic key-related information. This structure is similar to the architecture of subscriber authentication in wireless networks, and a reader seems like an access point (AP). However, the difference is that after successful authentication, the reader is not a mediator between an eSeal and the server any more, but it becomes a peer to the eSeal.

Based on the assumption that an eSeal and the central server share the 128-bit key (K) beforehand, our protocol will resort to a challenge-response mechanism using the standard symmetric cryptographic algorithm AES. We also assume that an eSeal and the reader have a pseudo-random number generator (PRNG), which is a reasonable assumption because a PRNG is required for various other purposes, for example, anti-collision.

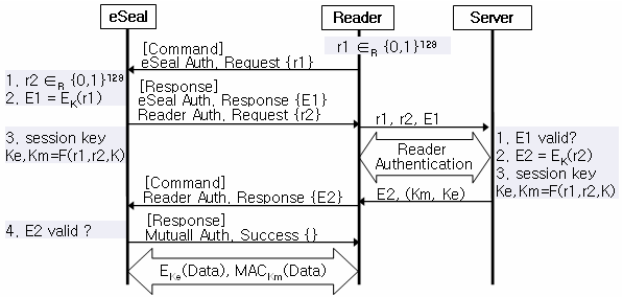

Fig. 2 Basic mutual authentication protocol

Before the authentication, the reader identifies the eSeal using the command defined in ISO 18185.

Then, the authentication protocol proceeds as follows.

1) Initially the reader generates a random value r1. The reader kicks off the authentication request using r1 as a challenge to authenticate the eSeal. This is implemented as a command from the reader to the eSeal.
2) After receiving challenge request, the eSeal computes the response $E1 = E_K(r1)$, and generates another random value r2 to authenticate the reader.
3) When the reader receives the eSeal's response, it requests the central server to authenticate the eSeal, sending the eSeal's response (r2,E1) with the seal ID retrieved from its access repository.
4) After authenticating the reader through a predefined secure channel, the central server authenticates the eSeal, and generates the response $E2 = E_K (r2)$. Next, the central server sends the result to the reader.
5) The reader just passes the response value (E2) to the eSeal, and the eSeal authenticates the central server, and thus the reader by checking the validity of response E2. That is, the eSeal confirms the authenticity of the reader via server authentication. At this point, mutual authentication process is completed.

6) While the mutual authentication is being processed, each party computes an encryption key Ke and a MAC key Km using a key derivation function F(), which uses r1, r2 and the master key K as input. Using these two kinds of new keys, it is possible for the reader and the eSeal to perform safe communication.

B. Improved Mutual Authentication Protocol

The above authentication protocol requires two rounds of command-response pairs. In this section, we present an improved protocol which requires only one round of communication. This improvement is based on the idea of the EAP-AKA protocol [13], which uses the AKA (Authentication and Key Agreement) mechanism defined in the 3GPP security architecture.

In the above protocol, both eSeal and server authentications are performed by challenge-response scheme using two random challenges (r1, r2). In the following protocol, by assuming that an eSeal and the central server share a sequence number (N) and another PRF (pseudo random function) G(), we can reduce the number of required challenges into only one per mutual authentication. Then the sequence number N plays the role of the second random value r2, and the eSeal doesn't need to generate the random value.

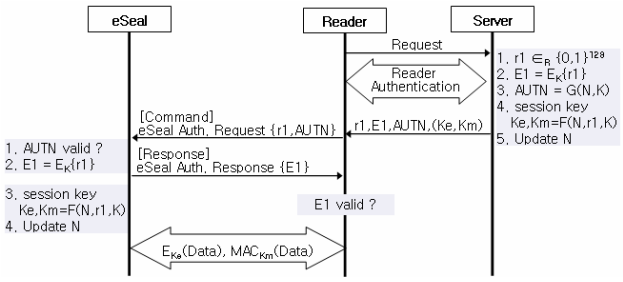

Fig. 3 Improved mutual authentication protocol

Like the previous protocol, after the reader identifies the eSeal using the command defined in ISO 18185, the authentication protocol proceeds as follows.

1) At first, the reader sends the request for eSeal authentication with the eSeal's identity to the central server.
2) After receiving the request, the central server computes AUTN using PRF G() and sequence number N. The server generates a random value r1 and computes 'E1=E_K(r1)'. Then, the server sends all of the computed values, i.e., AUTN, r1, and E1 to the reader.
3) The reader hands over AUTN and r1 to the eSeal, and stores E1.
4) The eSeal authenticates the reader by comparing the AUTN with the value computed by PRF G() in itself. Then, it computes E1 and sends it to the reader through the response message.
5) The reader verifies the response value E1 using the value stored in itself. Then mutual authentication is completed.
6) As in the first protocol, the new protocol enables two parties to share session keys (Ke, Km), which can be used encryption and message authentication.

V. Application to ISO 18185

A. Authentication Message Packet Formats

We organize the message packet formats for the second protocol, making it conform to ISO 18185 [5] as in Fig. 4.

B. Performance Evaluation

We simulate the communication between an eSeal and a reader using TI MSP430, flash based ultra-low-power 16-bit RISC MCU which operates up to 8MHz, and has 55~120KB program memory, 5~10KB SRAM, and about 2KB user memory. A test code for AES consumes 14KB Code, 4KB Data, and 10KB const (Priority is assigned to computation speed).

Table 1 shows the simulation results of AES operations under the target environment as above.

TABLE I
Simulation Results

Items		Value	Remarks
Memory		**28KB**	can be somewhat decreased
Comput-ation speed	AES_ ENCRYPT	3,353 cycles: 0.419 msec @8MHz	per 128 bits block
	AES_ DECRYPT	3,353 cycles: 0.419 msec @8MHz	per 128 bits block
	AES_ SET_KEY	29,815 cycles: 3.727 msec @8MHz	per one session

VI. Security Analysis

Under the assumptions on the eSeal system given in section III.C, we analyze the security features of our second protocol.

1) Mutual Authentication and Access Control:
Based on the feature of PRF (pseudo random function) G() and AES, the attacker cannot compute AUTN or the response value corresponding to challenge r1. So, our protocol prevents the attacker's impersonation and provides access control to eSeal.
2) Data Confidentiality:
Since master secret K is kept secret and the key derivation function F() is a PRF, the attacker cannot compute encryption key Ke. Then data confidentiality is guaranteed by this key and the AES algorithm.
3) Data Integrity:
Similarly, the security of the integrity key is guaranteed. So the MAC value guarantees the data integrity.
4) Data-Origin Authentication:
By comparing the MAC of decrypted value with received MAC value, a party can check if the data is changed or not. So our protocol guarantees the data-origin authentication.
5) Replay Protection:
In the basic authentication protocol, random numbers r1 and r2 is not reused, but are updated for each session. In the improved one, random number r1 and sequence number N are updated for each session, too. Therefore, the freshness of authentication messages is guaranteed.

[Command] eSeal Auth. Request {r1,AUTN}

Protocol ID	Packet Options	Tag Manufacture ID	Tag ID	Interrogator ID	Command Code	Min Command Duration*	Max Command Duration*	Argument Length	Command Arguments	CRC
0x80	0x0E	2 bytes	4 bytes	2 bytes	**0x72**	0x0000	0x7530	0x20(32)	**r1 || AUTN**	2 bytes

[Response] eSeal Auth. Response {E1}

Protocol ID	Seal Status	Packet Length	Interrogator ID	Tag Manufacture ID	Tag ID	Command Code	Data*	CRC
0x80	0x2800	0x1F(31)	2 bytes	2 bytes	4 bytes	**0x72**	**E_K (r1)**	2 bytes

Fig. 4 Improved mutual authentication message packet formats

REFERENCES

[1] World Shipping Council, International Mass Retail Association, and National Industrial Transportation League, "In-Transit Container Security Enhancement", 2003.09.09
[2] John F. Frittelli, CRS Report for Congress "Port and Maritime Security: Background and Issues for Congress", 2005.03.10.
[3] ISO/PAS 17712, "Freight containers - Mechanical seals", 2003.10.01
[4] Michael Wolfe, North River Consulting Group, "Electronic Cargo Seals: Context, Technologies, And Marketplace", 2002.07.12
[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 18185-4, "Freight containers - Electronic seals - Part 4:Data Protection", 2005.08.31
[9] ISO/DIS 18185-7, "Freight containers - Electronic seals - Part 7:Physical layer", 2005.04.28
[10] National Institute of Standards and Technology, FIPS PUB 197, "Advanced Encryption Standard (AES)", November 2001
[11] Motorola, Inc., "Second report of detailed container use cases and deficiencies in the ISO 18185-1, ISO 18185-7, and ISO 18000 standard", 2005.07.17
[12] National Institute of Standards and Technology, FIPS PUB 113, "Standard on Computer Data Authentication", May 1985.
[13] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", 2004.12.21