항만 물류 환경에서의 복제된 CSD 탐지를 위한 정책 기반 복제 탐지 매커니즘

황아름* · 서화정** · 김호원***

Policy Based Cloned CSD Detection Mechanism in Logistics

Ah-reum Hwang* · Hwa-jung Suh** · Ho-won Kim***

이 논문은 2011년도 부산대학교 차세대물류IT기술연구사업단 연구비를 지원받았음

요 약

컨테이너 보안 장치(CSD)는 컨테이너의 문 안에 장착되어 센서를 통해 컨테이너의 문이 비정상적으로 열리는 것을 탐지하는 장치다. 이러한 CSD 장치는 컨테이너의 보안성을 제공하는 장치이기 때문에 도청이나 위조와 같은 공격에 안전해야할 뿐만 아니라 복제 되어서도 안된다. 만약 복제된 CSD를 탐지할 수 없다면, CSD는 공격자에 의해 불법적으로 복제되어 정상적인 목적과는 다른 용도로 사용되어 질 수 있다. 본 논문에서는 이러한 복제된 CSD를 탐지하기 위한 정책 기반 복제 탐지 메커니즘을 제안한다. 또한 실제 구현 결과를 통해 제안하는 기법을 검증 및 평가한다.

ABSTRACT

CSD(Container Security Device) is a security device with sensors that can detect the abnormal behavior such as illegal opening of a container door. Since the CSD provides security and safety of the container, CSD should not only provide security services such as confidentiality and integrity but also cloning detection. If we can not detect the cloned CSD, an adversary can use the cloned CSD for many illegal purposes. In this paper, we propose a policy based cloned CSD detection mechanism. To evaluate proposed clone detection mechanism, we have implemented the proposed scheme and evaluated the results.

키워드

컨테이너 보안 장치, CSD, 복제 탐지 프로토콜, 정책 기반 복제 탐지, 복제 공격

Key word

Container Security Device, CSD, Clone Detect Protocol, Policy-based clone detect, Clone attack

* 준회원 : 부산대학교물류IT협동과정 석사과정
** 준회원 : 부산대학교 정보컴퓨터공학부 석사과정
*** 종신회원 : 부산대학교 정보컴퓨터공학부 교수
(교신저자, howonkim@pusan.ac.kr)

접수일자 : 2011. 11. 30
심사완료일자 : 2011. 12. 17

Ⅰ. 서 론

CSD는 Container Security Device[1]의 약자로, 컨테이너의 문 안 쪽에 부착되어 센서를 통해 문이 비정상적으로 열리는 것을 탐지하는 장치이며 능동형 RFID (Radio Frequency Identification) 태그의 일종이다. CSD 장치는 높은 보안성을 가지는 장치로서 컨테이너의 내용물에 대한 안전하고 신뢰할 수 있는 운송을 보장하는 장치다. 2007년 12월 미국 국토안보부 (DHS : Department of Homeland Security)에서는 CSD 요구사항 문서를 발표하였다[1]. 이 문서는 현재까지 CSD 표준으로 사용되어 지고 있으며, CSD의 보안과 관련된 요구 사항을 포함하고 있다. 하지만 실제 이 보안 요구 사항은 데이터 암호화에 대한 부분만 명시하고 있어서 여러 공격에 취약하다.

CSD는 컨테이너의 보안을 위해 만들어진 보안 장치임에도 불구하고 기본적으로 능동형 RFID 태그의특성을 가지므로 일반적인 능동형 RFID 태그에서 일어날 수 있는 도청, 위변조, 복제와 같은 공격이 있을 수 있다. 예로서 [2]에서는 RFID 태그를 위한 프라이버시 보호 기술에 대해 기술하고 있으며, 프라이버시 보호를 위한 Kill 태그, 패러데이 케이지 등 몇 가지 대표적인 기술을 소개하고 있다. 하지만, 이러한 RFID 프라이버시 보호 기술들은 반대로 RFID를 공격하는데 사용될 수도 있는 기술이다. 즉, 만약 패러데이 케이지 (Faraday cages)나 Jamming 기술을 사용하여 CSD와 게이트웨이의 통신을 차단 혹은 방해하면서 CSD를 복제하는 공격이 가능하다. 이와 같이 CSD에 대한 복제 공격은 실제 응용 환경에서 쉽게 발생할 수 있다.

[3, 4, 5]에서는 CSD와 같이 물류 환경에서 사용되는 RFID 태그를 위한 복제 탐지 기법을 제안하고 있다. 이 세 논문에서는 각 터미널 또는 항구들 사이의 이동 확률을 이용하여 복제를 탐지하는 방법을 제안하고 있지만, 이동 확률만을 사용하기 때문에 만약 공격자가 이동 확률을 비슷하게 맞추면서 복제된 태그를 사용하게 되면 이를 탐지할 수 없게 된다.

[6]에서는 CSD와 비슷한 전자봉인장치에서의 복제 공격에 대해 복제 방지 프로토콜을 제안하였다. 이 프로토콜은 [7]의 가변 식별자 태그 기법을 기반으로, 전자봉인장치의 이동 중에 값을 변화시킴으로써 복제를 방지하는 방법을 제안하고 있다. 하지만 CSD는 전자봉인장치에 비해 더 오래 사용되며 재사용이 가능한 점과 같이 전자봉인장치보다 더 복잡한 환경에서 사용되기 때문에 제안하고 있는 프로토콜은 CSD에 적합하지 않다.

본 논문에서는 복제된 CSD를 탐지하는 메커니즘을 제안하고 있다. 2장에서는 제안하는 프로토콜의 이해를 돕기 위해 CSD 시스템에 대해 설명한다. 3장에서는 제안하는 정책 기반 복제 탐지 기법에 대해 설명하고, 4장에서는 제안한 프로토콜의 구현 결과를 통해 성능을 제시한다. 결론에서는 논문의 기여 및 향후 연구 과제에 대해 설명한다.

Ⅱ. CSD 시스템

이 장에서는 제안하는 메커니즘의 관련 연구인 CSD 시스템에 대해 알아본다. [1]에서 설명된 CSD 시스템은 그림 1과 같다.

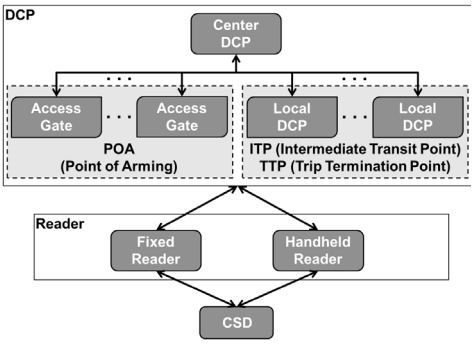

그림 1. CSD 시스템의 개요
Fig. 1 Overview of CSD system

CSD 시스템은 CSD, CSD와 DCP (Data Consolidation Point) 간에 데이터를 전달하고 CSD에게 명령을 보내는 리더, 그리고 서버인 DCP로 이루어져 있다.

CSD 리더는 두 가지 종류로 구성되는데, 하나는 각 항구 또는 터미널에 고정되어 있는 고정형 리더이고, 다른 하나는 컨테이너 운반자가 들고 다니는 이동형 리더이다. 리더와 CSD 간의 인터페이스와 각 계층에서의 통

1) 표준 문서에는 Coveyance Security Device로 정의되지만 실제 Container Security Device라는 용어가 많이 사용됨

신 프로토콜, 데이터 포맷 등에 대해서는 [8]에 자세히 설명되어 있다.

DCP는 중앙 DCP와 지역 DCP로 나뉘는데, 지역 DCP는 각 터미널 또는 항구에서 리더로부터 데이터를 읽어와 중앙 DCP에 넘겨주는 역할을 하고, 중앙 DCP는 모든 데이터들을 관리하고 외부 사용자에게 데이터를 제공해 주는 역할을 한다. DCP와 리더 간의 인터페이스와 통신 프로토콜, 메시지 타입과 예제 등에 대해서는 [9]에 자세히 설명되어 있다.

[1]에서는 CSD가 통과하는 터미널들을 세 가지로 나눠서 설명하고 있는데, POA(Point of Arming)는 CSD가 컨테이너에 장착되는 터미널이며, POA에서는 지역 DCP 대신 Access Gate가 사용된다. ITP(Intermediate Transit Point)는 POA와 마지막 도착지인 TTP(Trip Termination Point) 사이의 모든 터미널을 뜻하며, TTP는 CSD가 컨테이너로부터 탈착되는 도착지 터미널이다. 즉, CSD는 POA에서 컨테이너에 장착이 되며, 여러 ITP를 통과하여 TTP에서 탈착된다.

CSD는 각 POA, ITP, TTP를 드나들 때, 고정형 리더에 의해 데이터가 읽히게 되며, 각 터미널을 드나드는 시간이 중앙 DCP에 저장되어 진다.

Ⅲ. 제안하는 복제 탐지 메커니즘

이 장에서는 복제 탐지를 위해 제안하는 프로토콜에 대해 설명한다. 제안하는 프로토콜은 [6]에서 제안된 프로토콜을 기반으로 했는데 [6]에서는 CSD가 아닌 eSeal (Electronic Seal, 전자봉인장치)에서의 복제 탐지 기법을 제안하고 있으며 이 기법은 수입측과 수출측이 기존에 서로 주고받은 초기 값을 통해 만들어진 임의의 값 T를 사용하여 이동 중에 g(T)의 시간이 흐를 때마다 T 값을 계속해서 갱신하고 이후에 갱신된 최종 값을 계산함으로써 복제 여부를 검증하는 방법이다.

본 논문에서는 [6]의 방법을 기반으로 CSD의 환경에 더 적합하도록 [6]의 프로토콜을 수정하였으며 좀 더 복잡한 새로운 복제 검증 방법을 제안하고 있다. 특히, [6]에서는 복제 검증을 위해 이동 중에 갱신되었던 값만 확인을 하는 단순한 방식을 제안하고 있지만 본 논문에서는 CSD 시스템에 더 적합하도록 보다 복잡한 복제 검증 방법을 제안하고 있다.

프로토콜은 크게 세 가지로 구성된다. 첫 번째는 복제 탐지를 위해 필요한 값을 초기화하기 위한 초기화 프로토콜이고, 두 번째는 CSD가 이동하고 있을 때 복제를 방지하기 위해 초기화된 값을 갱신하는 N 값 갱신 프로토콜이며, 세 번째는 갱신된 값을 기반으로 CSD의 복제 여부를 확인하는 복제 여부 확인 프로토콜이다. 각 프로토콜에 대해서는 각 절에서 자세히 설명하겠다. 본 논문에서는 터미널 또는 항구를 모두 포인트라고 칭하며, 모든 프로토콜은 안전한 통신 채널에서 이루어진다고 가정한다.

3.1. 초기화 프로토콜

초기화 프로토콜은 복제 탐지를 위해 필요한 값들을 초기화시키는 프로토콜이며, POA와 ITP에서 이뤄진다. POA와 ITP에서 각각 비슷한 초기화 알고리즘이 행해지지만 사용되는 값이 조금씩 다르기 때문에 나눠서 설명한다.

POA에서는 화물주가 CSD를 컨테이너에 부착하고 활성화시키는 과정이 이뤄지며 POA에서의 초기화 프로토콜은 그림 2와 같다.

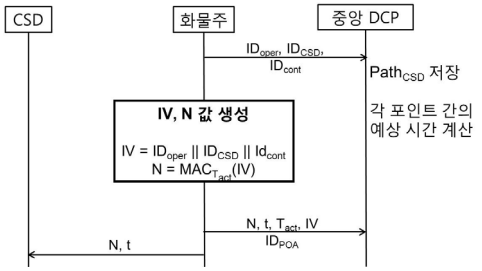

그림 2. POA에서의 초기화 과정
Fig. 2 Initialization process in POA

그림 2에서 보이는 과정은 다음과 같다.

1. 화물주는 사용자 인터페이스를 통해 중앙 DCP에게 자신의 아이디(IDoper)와 CSD의 아이디 IDCSD, 그리고 컨테이너의 아이디 IDCont를 중앙 DCP에 전달한다.
2. 중앙 DCP는 CSD가 이동할 경로(PathCSD)와 이동 경로의 각 포인트 간의 예상 시간을 계산해서 전달받은 값들과 함께 저장한다.

3. 화물주는 CSD를 활성화 시킨 후 이동 중에 필요한 값들을 다음과 같이 생성한다.

   $IV = ID_{oper} \| ID_{POA} \| ID_{Cont}$

   $N = MAC_{Tact}(IV)$
4. 화물주는 중앙 DCP에 N 값, IV 값, ID_{POA}, CSD가 활성화된 시간 T_{act} 값을 전달하고, CSD에는 N 값, 이후에 사용될 시간 t 값을 전달하는데, t 값은 화물주가 임의로 정한다.

ITP는 CSD가 TTP에 도달하기 전까지 지나가게 되는 포인트이며, CSD는 ITP에서 빠져 나올 때마다 POA에서 이루어졌던 것과 비슷한 초기화 과정을 거치게 된다. ITP에서의 초기화 과정은 그림 3과 같다.

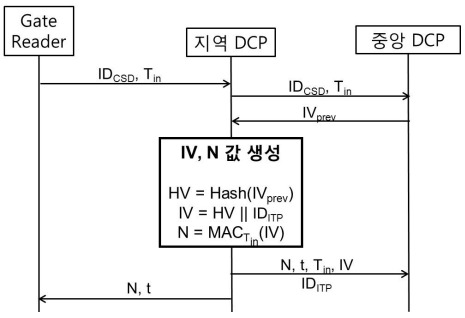

그림 3. ITP에서의 초기화 과정
Fig. 3 Initialization process in ITP

그림 3에서 보이는 과정은 다음과 같다.

1. CSD가 ITP에 도착해 게이트를 통과할 때, 게이트 리더는 CSD가 게이트를 통과한 시간 (T_{in})과 ID_{CSD}를 지역 DCP를 통해 중앙 DCP에게 전달한다.
2. 중앙 DCP는 해당 CSD의 이전 IV 값(IV_{prev})을 지역 DCP에게 전달한다.
3. 지역 DCP는 이동 중에 필요한 값들을 다음 과 같이 생성한다.

   $HV = Hash(IV_{prev}), IV = HV \| ID_{ITP}, N = MAC_{Tin}(IV)$
4. 지역 DCP는 N, IV 값과 CSD가 ITP의 게이 트에 들어온 시간 T_{in}, 이동 중에 N 값이 갱신될 시간 간격 값 t, 그리고 ITP의 아이디 ID_{ITP}를 중앙 DCP에 전달하고 CSD에는 N, t값을 전달한다.

POA와 ITP에서의 N 값 생성 과정의 다른 점은 IV 값을 생성하는 방식이다. POA에서는 IV 값을 ID_{oper}와 ID_{POA}, ID_{Cont}를 연결시켜서 생성했지만, ITP에서는 이전 IV 값에 해쉬함수를 취하고 다시 ID_{ITP}와 연결시켜서 IV 값을 생성한다.

3.2. N 값 갱신 프로토콜

N 값 갱신 프로토콜은 CSD가 포인트들 사이를 이동하는 중에 이루어지는 프로토콜로, 복제를 방지하기 위해 초기화 프로토콜 결과 값인 N 값을 t 시간마다 갱신하는 프로토콜이다. CSD가 포인트에서 다음 포인트로 이동하는 동안 N 값은 일정 시간 t마다 다음 식과 같이 이전 N 값에 해쉬 함수를 취해 N(Hash())값을 계속해서 갱신하게 된다.

이는 공격자가 공격을 해서 N 값을 취하게 되더라도 이후에 중앙 DCP가 계산을 하면서 N 값을 비교해 봄으로써, 복제를 탐지할 때 사용하기 위함이다.

3.3. 복제 여부 확인 프로토콜

복제 여부 확인 프로토콜은 ITP와 TTP에 CSD가 들어올 때마다 CSD의 복제 여부를 확인하기 위한 프로토콜이다. CSD가 각 ITP 또는 TTP의 게이트를 통과할 때 고정형 리더는 CSD로부터 CSD ID와 이벤트 로그뿐만 아니라, 이전 포인트 ID, 현재 N 값, 데이터를 읽은 시간을 지역 DCP에 전달하고 지역 DCP는 CSD의 복제 여부를 3가지 방법을 통해 확인하게 되며 이 때 복제 여부 판단은 사용자가 미리 정해 놓은 정책에 따른다. 이것은 DCP가 사람처럼 스스로 판단하여 복제 여부를 결정할 수 없기 때문에 사용자가 미리 복제라고 판단되는 경우를 정책으로 정해 놓고 DCP는 이 정책에 따라 복제 여부를 판단하여 사용자에게 알리기 위함이다.

CSD 복제 여부 확인을 위한 첫 번째 방법은 저장된 이동 경로와 현재 이동 경로 대조를 통해 복제 여부를 확인하는 CSD 이동 경로 기반 복제 여부 확인 방법으로, 그림 4와 같다.

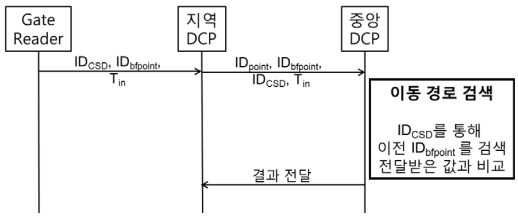

그림 4. 이동 경로 기반 복제 여부 확인 프로토콜 과정
Fig. 4 Cloning detection protocol based on CSD's path

그림 4에서 발생되는 과정은 다음과 같다.

1. 게이트 리더는 지역 DCP를 통해 중앙 DCP 에게 현재 포인트의 아이디와 CSD에 저장되어 있는 이전 포인트의 아이디를 전달한다.
2. 중앙 DCP는 화물 운반자가 저장해 뒀던 컨 테이너의 이동 경로에서 현재 포인트 아이디 (ID_{point})의 이전 포인트 아이디를 검색한다.
3. 검색된 아이디가 CSD가 전달해 준 이전 포 인트의 아이디 $ID_{bfpoint}$와 다르면 복제 가능성이 있다고 판단한다.

이 프로토콜의 경우에는 전혀 엉뚱한 포인트로 이동한 CSD를 탐지하게 된다. CSD 복제 여부 확인을 위한 두 번째 방법은 저장된 각 포인트 간 이동 예상 시간과 실제 이동 시간 대조를 통해 복제 여부를 확인하는 예상 시간 기반 복제 여부 확인으로, 그림 5와 같으며 그림 5에서 발생하는 과정은 다음과 같다.

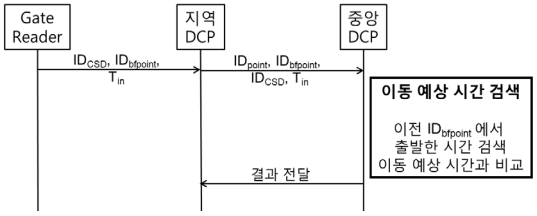

그림 5. 예상 시간 기반 복제 여부 확인 프로토콜 과정
Fig. 5 Cloning detection protocol based on expected time

1. 게이트 리더는 지역 DCP를 통해 중앙 DCP 에게 현재 포인트의 아이디, 이전 포인트의 아이디, 게이트에 들어온 시간을 전달한다.
2. 중앙 DCP는 CSD가 이전 포인트에서 출발한 시간을 검색하고 CSD가 실제 이동한 시간 T_{mov}을 계산한다.
3. 중앙 DCP는 현재 포인트와 이전 포인트 간 의 예상 이동 시간 T_{exp}을 검색한 뒤 T_{mov}와 T_{exp} 간의 차이를 계산한다.
4. 만약 계산된 차이 값이 보안 에이전트가 미 리 정해 뒀던 ±α 값 범위를 벗어나면 복제가 되었다고 판단한다.

이 프로토콜은 정해진 경로대로 움직였더라도 예상 시간 내에 도착하지 못할 경우를 탐지해 내게 된다. 여기서 α 값은 보안 에이전트에 의해 임의로 정해지는 값인데 실제 이동 시에 생길 여러 상황들을 고려해서 정하는 것이 중요하다. CSD 복제 여부 확인을 위한 세 번째 방법은 초기화 프로토콜에서 생성되어서 이동 중에 갱신되었던 N 값을 계산된 N 값과의 대조를 통해 복제 여부를 확인하는 N 값 기반 복제 여부 확인 방법으로, 그림 6과 같다.

1. 게이트 리더는 지역 DCP를 통해 중앙 DCP 에게 CSD, N 값 등을 전달한다.
2. 중앙 DCP는 CSD가 이전 포인트에서 출발한 시간 $T_{bfpoint}$와 CSD가 현재 포인트의 게이트를 통과한 시간 T_{in}을 통해 CSD가 이동한 시간을 계산한 뒤 이동 중에 몇 번의 갱신이 이루어 졌는지 계산한다.

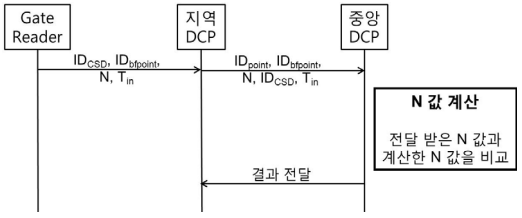

그림 6. N 값 기반 복제 여부 확인 프로토콜 과정
Fig. 6 Cloning detection protocol based on value N

3. 중앙 DCP는 이전 포인트에서 생성해서 저장된 N 값을 검색해서 n만큼 갱신을 해서 새로운 N′ 값을 계산한다.
4. 중앙 DCP는 CSD로부터 전달받은 N 값과 계산된 새로운 N′값을 비교해서 만약 두 값이 틀리면 복제가 되었다고 판단한다. 이 프로토콜의 경우에는 이동 중에 CSD가 복제가 되는 것을 탐지하기 위해 N이라는 값

을 통해 복제 여부를 판단하는 프로토콜이다. 중간에 공격자가 CSD를 복제할 경우 N 값이 달라지게 되면 이를 탐지할 수 있게 된다.

Ⅳ. 제안 메커니즘 구현 및 결과

4.1. 구현 방법

본 논문에서는 실제 환경인 POA, ITP, TTP에서 실험을 할 수 없었기 때문에 시뮬레이션을 통해 제안한 복제 탐지 메커니즘의 성능을 제시한다. 시뮬레이션은 그림 7과 같이 C#으로 구현한 웹 형태의 프로그램이며 사용자 관리 프로그램 형태로 구현되었다. MS SQL을 이용하여 구현된 DB는 DCP를 대신하는데, 시뮬레이션이기 때문에 중앙 DCP와 지역 DCP를 분리하지 않고 통합해 나타냈다. 즉, 리더를 거치지 않고 CSD와 DCP가 직접 연결된 구조라고 말할 수 있다. 시뮬레이션은 CSD 데이터를 생성해서 DB에 저장하는데 이 때 표 1과 같이 몇 가지 시나리오가 반영된 데이터가 생성되어서 DB에 저장된다.

그림 7. 시뮬레이션 프로그램 화면
Fig. 7 Screen View of Simulation program

표 1. 시뮬레이션에 사용된 시나리오
Table. 1 Scenarios in simulation

시나리오 1	CSD가 path에 맞게 이동, 예상 시간 안에 각 포인트 도착, 올바른 N 값을 가진 정상적인 시나리오
시나리오 2	CSD가 path에 맞게 이동, 예상 시간과 다르게 포인트에 도착한 비정상적인 시나리오
시나리오 3	CSD가 path에 맞게 이동, 예상 시간 안에 각 포인트 도착, 올바르지 않은 N 값을 가진 비정상적인 시나리오

시뮬레이션은 DB에 저장된 현재 사용되고 있는 CSD의 ID에 대해 표 1과 같이 복제 여부를 3단계로 나눠서 판단하는데, 이 복제 여부 판별 단계는 앞에서 제안한 복제 여부 확인 프로토콜의 결과를 통해 결정되며 미리 정해 놓은 정책에 따라 세 가지 단계 중 한 가지로 결정된다. 초기화 프로토콜에서 사용된 MAC 함수와 Hash 함수는 HMAC과 SHA-1을 사용하였다.

표 2. 복제 여부 판별 단계
Table. 2 Level of verification

단계 1	Dangerous Level: 복제가 확실하다고 여겨지는 경우, N 값과 이동 경로가 잘못된 경우에 이 단계로 판별
단계 2	Doubtful Level: 복제일 수도 있다고 여겨지는 경우, 이동 시간이 예상 시간과 다를 경우에 이 단계로 판별
단계 3	Safe Level: 복제가 되지 않은 안전한 경우

4.2. 구현 결과

4.2.1. 복제 탐지 메커니즘이 적용되지 않은 경우

이 절에서는 먼저 복제 탐지 메커니즘이 적용되지 않은 일반적인 경우를 보인다. 그림 5는 복제 탐지 메커니즘이 적용되지 않은 경우의 시뮬레이션 화면으로, 복제 탐지 메커니즘이 적용되지 않은 경우 시뮬레이션은 아주 간단한 정보만을 사용자에게 제공해 주고 있다.

복제 탐지 메커니즘이 적용되지 않은 일반적인 경우

CSD ID	Current Loc	Read Date
AS2356S5S8	홍콩	2011-07-07 오후 1:34:49
WF2565D3Q2	시애틀	2011-08-16 오후 7:00:09
WA2325W2S3	시애틀	2011-04-03 오전 11:16:19
HC3546A2S3	아우토반	2011-09-15 오전 4:27:57
EW3215F3Z2	아우토반	2011-04-02 오전 10:37:56
WA5621V2W3	아우토반	2011-08-09 오전 11:57:24
EV2536S5D5	부산	2011-09-10 오전 9:27:36
AS2356S5S8	오키나와	2011-07-07 오전 6:25:34
WF2565D3Q2	오클랜드	2011-08-16 오후 12:15:25
HC3546A2S3	브레멘	2011-09-12 오후 4:34:19

1 2 3

그림 8. 일반적인 사용자 화면의 CSD 정보
Fig. 8 Information of CSD in general user screen

예를 들면, 사용자는 그림 8과 같이 사용되는 CSD의 아이디와 현재 포인트, CSD가 게이트 리더에 읽힌 시간

등 간단한 정보만 확인할 수 있는데, 그림 8의 리스트에는 실제로 정상적인 CSD도 있지만 복제되었거나 복제되었다고 의심되는 CSD도 있다. 그림 8의 리스트에서 세 번째에 위치한 ID가 WA2325W2S3인 CSD의 경우 서버에 저장된 경로 정보에 따르면 현재 포인트인 시애틀 항에 오기 전에 오키나와 항에서 출발을 했어야 했지만 오키나와 항이 아닌 안트워프 항에서 출발을 했다. 하지만 사용자는 해당 정보를 확인할 수 없다. 그림 8의 리스트에서 다섯 번째에 위치한 ID가 EW3215F3Z2인 CSD의 경우 이전 포인트인 안트워프 항에서 현재 포인트인 아우토반 항까지 7080분에서 7920분 사이에 도착 예정이지만 실제 걸린 시간은 7000분으로 80분이나 빨리 도착을 했다. 이 경우 실제로는 공격자가 CSD를 복제해 안트워프 항에서 출발한 것처럼 정보를 넣고 CSD를 다른 항구에서 아우토반 항으로 보냈을 가능성도 있고, 또는 특정한 사유가 있어 예상 시간보다 빨리 도착했을 수도 있지만 사용자는 이와 같은 정보를 확인할 수가 없다.

4.2.2. 복제 탐지 메커니즘이 적용된 경우

그림 8에서 보인 것과 같은 데이터에 복제 탐지 메커니즘을 적용한 경우의 결과가 그림 9에 나타나 있다.

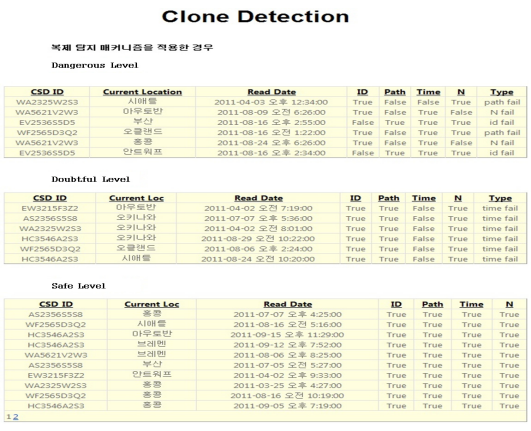

그림 9. 복제 탐지 메커니즘이 적용된 사용자 화면의 CSD 정보
Fig. 9 Information of CSD with clone detection mechanism in user screen

그림 9에서는 CSD의 정보를 하나의 리스트에서 보여주던 그림 8와는 다르게 표 2의 복제 여부 판별 단계에 따라 CSD 리스트를 나누어서 사용자에게 한 화면에서 결과를 보여 주고 있다. 첫 번째 리스트는 Dangerous Level 리스트로 표 2의 단계 1로 판별된 CSD를 보여 주고 있는데, Path가 잘못되었거나 계산된 N 값이 예상되는 N 값과 다를 경우가 단계 1로 판별이 되며 N 값이 틀릴 경우에 "N fail"이라는 결론을, Path가 틀릴 경우에 "path fail"이라는 결론을 Type 칸에 보여 주고 있다. 두 번째 리스트는 Doubtful Level 리스트로 표 2의 단계 2로 판별된 CSD를 보여 주고 있는데, 도착 시간이 예상 시간 범위를 벗어난 경우가 단계 2로 판별이 되며 "time fail"이라는 결론을 Type 칸에 보여 주고 있다. 세 번째 리스트는 Safe Level 리스트로 표 2의 단계 3으로 판별된 CSD를 보여 주고 있는데, Path, 도착 시간, N 값에 대한 결과가 모두 True로 판별된 안전한 CSD만을 보여 주고 있다. 그림 9에서는 복제가 확실하다고 판별되는 단계 1과 복제 가능성이 있다고 판별되는 단계 2의 경우에 해당 CSD가 단계 1과 2로 판별된 이유에 대해서도 함께 보이고 있기 때문에 사용자는 화면에서 즉각적으로 CSD의 상태를 확인할 수 있게 되며, 또한 단계 1과 2의 리스트에 올라와 있는 CSD들의 상태에 대해서만 바로 체크해 보면 되기 때문에 복제된 CSD에 대해 즉각적으로 대처할 수 있다. 예를 들면, 그림 8의 리스트에서 세 번째에 위치했던 ID가 WA2325W2S3인 CSD는 그림 9의 Dangerous Level 리스트에서 첫 번째에 위치해 있는데, 그림 8에서는 해당 CSD가 잘못된 경로를 통해 이동 중인 것을 사용자가 확인할 수 없었지만 그림 9에서는 해당 CSD를 Dangerous Level 의 리스트에서 바로 확인함으로써 복제되었다는 것을 바로 알 수 있을 뿐만 아니라, 해당 CSD의 Path와 time의 복제 여부 확인 결과가 False로 나타난 것을 확인할 수 있기 때문에 이에 대해서 빠르게 대처할 수 있다.

그림 8의 리스트에서 다섯 번째에 위치했던 ID가 EW3215F3Z2는 그림 9의 Doubtful Level 리스트에서 첫 번째에 위치해 있는데, 그림 8에서는 CSD가 현재 포인트에 예상 시간보다 빨리 도착한 것을 사용자가 확인할 수 없었지만 그림 9에서는 해당 CSD의 time의 복제 여부 확인 결과가 False로 나타난 것을 확인할 수 있기 때문에 이에 대해서 바로 확인해 볼 수 있다. 그림 8와 그림 9을 비교해 보면 같은 데이터에 대해서 그림 8는 사용자에게 단순한 정보만을 제공해 주고 있기 때문에 사용자는 CSD의 상태를 정확하게 판단할 수가 없지만, 그

림 9는 저장되어 있는 데이터에 대해 복제 여부를 확인하고 이에 대한 결과를 복제 여부 단계별로 나눠서 사용자에게 보여줌으로써 사용자가 복제되거나 의심이 가는 CSD를 바로 알아 볼 수 있도록 하였다. 또한, 사용자에게 보다 정확한 CSD의 상태를 제공해 주고 있기 때문에 사용자는 더 정확한 CSD의 상태를 알 수 있다. 즉, 사용자는 CSD의 상태를 빠르고 쉽게 확인해서 해당 CSD의 상태를 직접 확인하고 복제된 CSD를 빠르게 폐기 처분할 수 있기 때문에 보다 안전하게 CSD를 사용할 수 있게 된다.

4.3. 프로토콜 동작 검증

만약 공격자가 어떠한 방법으로 이동 중인 CSD에 저장되어 있는 N과 t 값, 이전 포인트 ID를 알아낸다고 가정할 경우, 공격자는 얻어낸 값들을 이용해 정상적인 CSD처럼 복제할 수 있다. 공격자는 복제된 CSD를 사용하여 제안한 복제 탐지 메커니즘을 통과하기 위해서 복제 여부 확인 프로토콜의 세 가지 방법을 통과해야 한다. 하지만 CSD는 N과 t 값, 이전 포인트 ID 외에 복제 여부 확인 프로토콜에서 사용되는 다른 데이터를 저장하고 있지 않기 때문에 공격자는 제안한 복제 탐지 메커니즘을 통과할 수가 없다. 만약 공격자가 제안한 복제 탐지 메커니즘을 통과하려면 다음과 같이 많은 데이터를 미리 알고 있어야 한다. 공격자는 복제 여부 확인 프로토콜의 첫 번째 방법인 이동 경로 기반 복제 여부 확인 방법을 통과하기 위해서 해당 CSD의 화물주 ID를 알고 있어야 하며, 화물주가 DCP에 저장한 CSD의 이동 경로와 다음 포인트를 알고 있어야 이동 경로 기반 복제 여부 확인 방법을 통과할 수 있다.

공격자는 복제 여부 확인 프로토콜의 두 번째 방법인 예상 시간 기반 복제 여부 확인 방법을 통과하기 위해서 해당 CSD의 이동 예상 시간 범위와 이전 포인트에서 출발한 시간을 알고 있어야 하며, 예상 시간 범위 안에 다음 포인트에 도착을 해야 예상 시간 기반 복제 여부 확인 방법을 통과할 수 있다. 공격자는 복제 여부 확인 프로토콜의 세 번째 방법인 N 값 기반 복제 여부 확인 방법을 통과하기 위해서 해당 CSD의 N 값을 얻어낸 순간의 N 값이 몇 번의 해쉬 함수를 취한 값인지를 알고 있어야 하며, t 시간마다 계속적으로 N 값에 해쉬 함수를 취해 N 값을 갱신해야 다음 포인트에 도착해서 N 값 기반 복제 여부 확인 방법을 통과할 수 있다. 따라서 제안한 복제 탐지 메커니즘은 사용자가 미리 정해 놓은 정책에 따라 다각적인 방면에서 복제 여부를 확인하기 때문에 공격자가 쉽게 공격에 성공할 수가 없다.

V. 결 론

본 논문에서는 CSD의 복제 공격에 대해 정책적으로 복제된 CSD를 탐지해 낼 수 있는 정책 기반 복제 탐지 메커니즘을 제안하고 있다. 복제된 CSD를 탐지하기 위해서 화물주가 CSD의 이동 경로를 저장하고 DCP에서는 저장된 경로를 통해 각 포인트 간의 예상 시간을 계산해서 저장하게 했으며, 특정한 값을 사용하여 이 값이 컨테이너가 이동하는 동안 일정시간마다 갱신되도록 하였다. DCP는 이렇게 저장된 값들을 사용하여 CSD가 각 포인트에 도착할 때마다 CSD의 이동 경로, 이동 시간, 갱신된 값을 확인하여 CSD의 복제 여부를 확인한 뒤 미리 정해둔 정책에 따라 복제 여부를 판단하게 함으로써 DCP가 스스로 복제된 CSD를 탐지하여 사용자에게 알리도록 하였다. 제안한 메커니즘을 검증하기 위해 시뮬레이션 프로그램을 구현하여 예상되는 시나리오대로 데이터를 생성하고 메커니즘을 적용시켜서 메커니즘이 적용되지 않은 일반적인 경우와 비교해 봄으로써 본 제안 프로토콜의 동작을 검증할 수 있었다. 본 논문에서는 제안하는 복제 탐지 메커니즘에 대해 시뮬레이션을 통한 실험만을 진행하였지만 향후 실제 환경에서 실험을 진행할 계획이며 더욱 다양한 복제 시나리오에 대한 대응 연구도 진행할 예정이다.

참고문헌

[1] Conveyance Security Device (CSD) Requirement Document Baseline version 1.2, December 10, 2007

[2] 이향진, 신동휘, 전길수, “RFID 프라이버시 보호 기술 및 표준화 동향”, 정보보호학회지 제 18권 제4호, 2008.8

[3] Mikko Lehtonen, Florian Michahelles, and Elgar Fleisch, ″How to Detect Cloned Tags in a Reliable Way from Incomplete RFID Traces″, 2009 IEEE International Conference on RFID, pp.257-264, April

27-28, 2009

[4] Mikko Lehtonen, Daniel Ostojic, Alexander Ilic, and Florian Michahelles, "Securing RFID Systems by Detecting Tag Cloning", Lecture Notes in Computer Science, vol. 5538, pp.291-308, Springer, 2009

[5] Davide Zanetti, Leo Fellmann, and Srdjan, "Privacy-preserving Clone Detection for RFID-enabled Supply Chains", 2010 IEEE International Conference on RFID, pp.37-44, April 14-16, 2010

[6] 김주해, 최은영, 이동훈, "복제 공격 저항성을 갖는 전자봉인 보안 모델", 정보보호학회논문지 제 17권 제5호, pp.111-116, Oct, 2007

[7] D.Henrici and Paul Muller, "Hash-based enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", PerSec'04 at IEEE PerCom, pp.149-153, 2004

[8] Conveyance Security Device (CSD)-to-CSD Reader Interface Control Document (ICD) Baseline version 1.0, December 10, 2007

[9] CSD Reader-to-Data Consolidation Point (DCP) Interface Control Document (ICD) Baseline version 1.0, December 10, 2007

저자소개

황아름(Ah-reum Hwang)

2006.3 ~ 2010.2 : 부산대학교 정보컴퓨터 공학과 학사
2010.3 ~ 현재 : 부산대학교 물류 IT협동과정 석사

※관심분야 : CSD 보안, 부채널 공격

서화정(Hwa-jeong Seo)

2004.3 ~ 2010.2 : 부산대학교 정보컴퓨터공학과 학사
2010.2 ~ 현재 : 부산대학교 컴퓨터공학부 석사

※관심분야 : 정보보안, RFID/USN, 암호 이론, VLSI

김호원(Ho-won Kim)

1989. 3 ~ 1993. 2 : 경북대학교 전자공학과 학사
1993. 3 ~ 1995. 2 : 포항공과대학교 전자전기공학과 공학석사
1995. 2 ~ 1999 .2 : 포항공과대학교 전자전기공학과 공학박사
1998.12~ 2008. 2 : 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원 / 팀장
2008. 3 ~ 현재 : 부산대학교 정보컴퓨터공학부 부교수

※관심분야 : 스마트그리드 보안, RFID/USN 보안, PKC 암호, VLSI, Embedded system 보안