중계 공격 대응을 위한 차량 문 개폐 시스템에 대한 연구

민정기*, 최원빈*, 김승주*
*고려대학교 정보보호대학원
e-mail:eternalray123@gmail.com

A Study on Car Door Open/Lock System Preventing Relay Attack

Jungki Min*, Wonbin Choi*, Seungjoo Kim*
*Center for Information Security Technologies(CIST), Korea University.

요 약

스마트폰 키 애플리케이션이 널리 사용되면서, 이에 대한 중계 공격의 위협도 증가하고 있다. 중계 공격은 공격자가 차량과 키 애플리케이션 사이에서 오고가는 신호를 중계하여 허용 범위 밖의 통신을 시스템이 유효한 것으로 판단하게 하는 공격이다. 본 논문에서는 중계 공격을 막기 위해, 추가 지연 시간을 탐지하여, 임계 지연 시간을 넘었을 경우 차량과 스마트키가 충분히 근접하지 않았다고 판단하여 차량 문 개폐 요청을 거부하는 시스템을 제안하였다. 또한 실제 환경에서의 유동성을 고려하여 임계 지연 시간을 지속적으로 업데이트하는 적응 임계 지연 시간(Adaptive Delay Threshold) 기술을 제시하였다. 그리고 실제 임베디드 기기를 이용해 시스템을 구현하여 시스템의 실효성을 검증하였다.

1. 서론

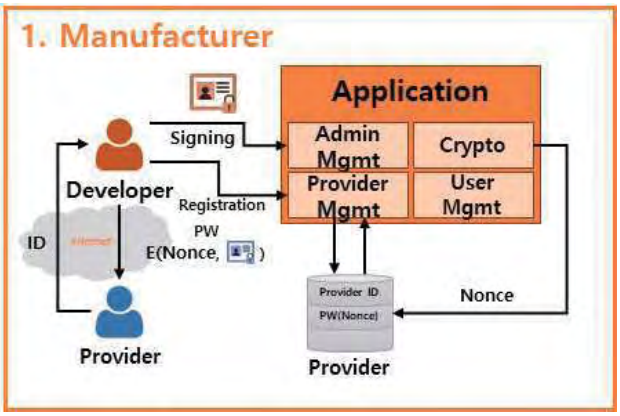
최근 차량 사용의 편의를 위해, 키를 소지하지 않더라도 차량 문을 열고 닫을 수 있는 스마트폰 키 애플리케이션이 널리 사용되고 있다. 대표적으로 국내에서 널리 사용되는 차량 공유 서비스인 쏘카는 등록된 차량을 대여하여 스마트폰 애플리케이션을 통해 차량 내부를 제어할 수 있을 뿐만 아니라, 원격으로 차량 문을 열고 닫을 수 있다. 또한 외국에서 서비스중인 Car Chabi는 스마트폰 애플리케이션 서비스로, 차량 내부에 센서를 장착하고 센서와 애플리케이션간의 블루투스 통신을 통해 원격 차량 문 개폐 기능을 제공한다.

키 애플리케이션이 널리 사용됨에 따라, 이러한 애플리케이션을 이용하는 차량 문 원격 개폐 시스템을 대상으로 하는 중계 공격의 위협이 증가하고 있다. 중계 공격[1][2]이란, 차량과 키 애플리케이션 사이의 문 개폐 신호를 공격자가 중간에서 중계하여, 사용자가 통신 허용 범위 밖에 있더라도 차량과 정상적으로 통신하여 차량 문을 개폐하는 공격이다. 중계 공격은 공격자가 신호 자체의 내용을 해독할 필요 없이, 그저 중간에서 오고 가는 신호를 중계하기만 하면 되기 때문에, 신호가 암호화 되어 있다 하더라도 유효한 공격 방법이다. 그러나 허용 범위 밖까지 신호를 중계하기 위해서는 증폭기를 이용해 신호를 증폭시키거나 중간 단계의 프록시 기기를 이용해 신호를 중계해야하므로, 이 과정에서 추가적인 지연 시간이 발생한다. 이러한 추가적인 지연시간을 탐지함으로써 중계 공격이 발생했는지 여부를 확인할 수 있다.[3]

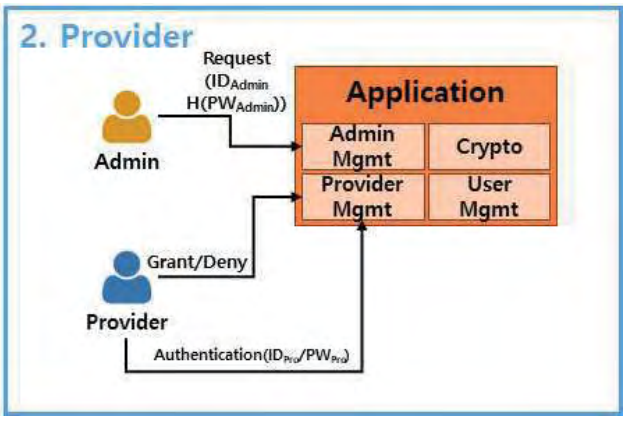
본 논문에서는 지연 시간을 기반으로 차량과 사용자가 충분히 근접했는지를 판단하고, 이를 기반으로 중계 공격 여부를 확인하여 차량 문 개폐 허용 및 거부를 결정하는 차량 문 개폐 시스템을 제안한다. 그리고 실제 환경에서의 지연 시간의 유동성을 고려하여 임계 지연 시간을 계속해서 업데이트하는 적응 임계 지연 시간 알고리즘을 제시한다. 또한 이 시스템을 직접 임베디드 기기를 이용해 구현하여, 차량 문 개폐 인증 정확도를 측정하였다.

이 논문은 2018년도 정보(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(R7117-16-0161, 자율주행 스마트자동차용 이상징후 탐지핵심기술개발)

2. 차량 문 개폐 시스템 구조



(그림 1) 제조사 도메인 구조

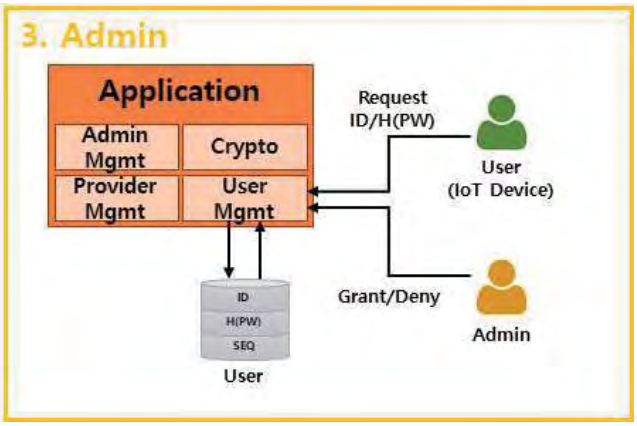


(그림 2) 판매자 도메인 구조

(그림 1)은 제조사(Manufacturer) 도메인의 구조를 나타낸다. 우선 시스템 제조사는 전자 서명을 이용해 판매자에게 자신이 정말 시스템 제조사가 맞는지를 인증한다. 그다음 판매자가 판매자 계정 생성을 요청하면, 넌스(Nonce) 값을 이용해 패스워드를 생성한 후 판매자의 공개키로 패스워드를 암호화한다. 그 후 인터넷을 통해 암호화 된 패스워드를 판매자에게 보내주고 해당 판매자를 판매자 데이터베이스에 등록한다. 이를 통해 제조사는 자신의 시스템을 판매할 판매자를 관리할 수 있다.

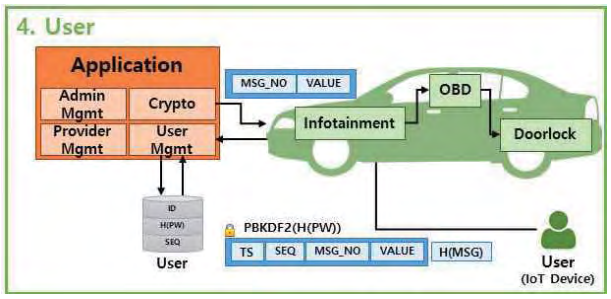
(그림 2)는 판매자(Provider) 도메인의 구조를 나타낸다. 판매자는 암호화 된 패스워드를 자신의 개인키로 복호화하여, 관리자와 사용자 계정을 생성, 관리할 수 있는 판매자 계정을 사용할 수 있게 된다. 판매자는 이러한 판매자 계정을 이용하여 시스템을 구매한 차량 주인에게 관리자 계정을 생성해주고, 관리자의 차량 관리 권한을 인가해준다. 또한 이를 관리자 데이터베이스에 등록하여 관리한다. 실제 환경에서는 이러한 과정이 판매 매장과 같은 오프라인에서 이뤄지므로, 판매자와 관리자간의 인증 문제가 해결된다. 또한 관리자 계정이 도난당할 경우를 대비하여 차량 관리 권한을 회수 할 수도 있다.

(그림 3)은 관리자(Admin) 도메인의 구조를 나타낸다. 차량의 관리자는 자신이 추가적으로 차량 문 개폐 시스템 사용을 허락할 사용자들에게 계정을 생성해 주고, 이를 사용자 데이터베이스에 등록하여 관리한다. 관리자는 사용자들에게 차량 문 개폐 권한을 부여하거나 회수할 수 있다. 권한을 받은 사용자는 차량 문을 개폐 할 수는 있지만, 다른 사용자의 권한에 영향을 미칠 수 없다.



(그림 3) 관리자 도메인

(그림 4)는 사용자(User) 도메인의 구조를 나타낸다. 사용자는 키 역할을 하는 IoT 기기에 설치된 클라이언트 프로그램과, 차량 인포테인먼트에 설치된 서버 프로그램의 통신을 통해 차량 문을 개폐할 수 있게 된다. 사용자는 차량에게 타임스탬프, 시퀀스 번호, 메시지 번호, 메시지 값을 NIST 800-132 표준[4]에 기술된 PBKDF(Password-Based Key Derivation Function)2 알고리즘을 사용하여 사용자 계정의 패스워드로 유도된 대칭키를 이용해 암호화 하여 보낸다. 시퀀스 번호는 재전송 공격을 막기 위한 필드로, 시퀀스 번호가 없을 경우 공격자가 신호를 도청 해두었다가 이를 재전송하여 차량 문을 개폐할 수 있게 된다. 메시지 번호는 특정 명령을 수행하기 위한 번호로, 현재 시스템에서는 차량 문 개폐 신호만을 사용하기 때문에 고정된 값이다. 메시지 값은 해당 명령에 대한 인자 값으로, 차량 문을 열 때는 0, 닫을 때는 1이다. 타임스탬프 값은 중계 공격을 막기 위한 필드 값으로, 인포테인먼트에 설치된 서버 프로그램이 IoT 기기에 설치된 클라이언트 프로그램으로부터 받은 신호의 타임스탬프 값을 보고 신호 전달 지연 시간을 계산한다. 만약 신호 전달 지연 시간이 임계 지연 시간 보다 클 경우, 차량과 사용자가 충분히 근접하지 않았다고 판단해 차량 문 개폐가 허가되지 않는다.



(그림 4) 사용자 도메인 구조

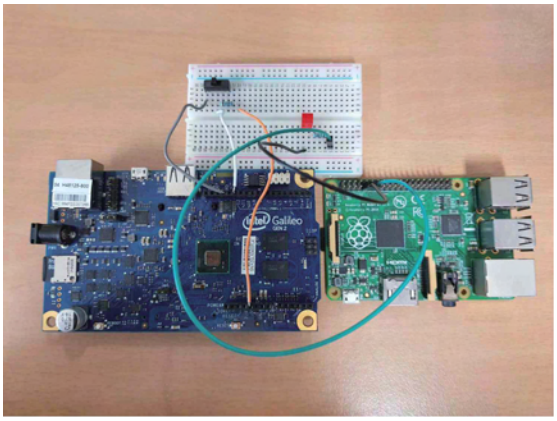
```
GLOBAL : T, r[k]
adaptiveDoorCheck(t)
  a ← false
  if t <= T
    then a ← true

  dequeue(r)
  enqueue(t,r)

  b ← mean(r)
  c ← standard_deviation(r)
  T ← b + 2.5 x c

  return a
end
```

용어	설명
t	입력으로 받은 신호의 전달 지연 시간
T	임계 지연 시간
r[k]	이전 신호 지연 시간을 저장하고 있는 사이즈 k인 큐

(그림 5) 적응 임계 지연 시간을 적용한 알고리즘의 의사 코드

임계 지연 시간을 정하는 방법에는 크게 두가지가 있다. 첫번째는 고정된 임계 지연 시간 값을 사용하는 것이다. 이 방법은 간단하고 구현하기가 편리하지만, 실제 환경에 따라 지연 시간이 유동적으로 바뀌는 경우에 시스템이 정상적으로 작동하기 힘들다는 단점이 있다. 이러한 실제 환경의 유동성을 고려한 두번째 방법은 바로 임계 지연 시간을 지속적으로 업데이트하는 것이다. 임계 지연 시간을 상황에 맞춰 적응시켜 나가는 적응 임계 지연 시간(Adaptive Delay Threshold)은 실제 상황에서 지연 시간이 상황에 따라 바뀔 때에도 그에 따라 임계 지연 시간을 유동적으로 업데이트하여 사용할 수 있다는 장점이 있다. (그림 5)는 적응 임계 지연 시간을 적용한 차량 문 개폐 허용 알고리즘의 의사코드를 나타낸다. 알고리즘은 전달받은 신호의 지연 시간 t를 입력으로 받아 임계 지연 시간 T와 비교하여 요청을 허가하거나 거부한다. 여기까지는 고정 임계 지연 시간을 사용하는 경우와 같다. 그러나 추가적으로, 이전에 전달받은 신호의 지연 시간을 k개만큼 큐에 저장하고 있다가 입력 받은 지연 시간 t와 가장 오래된 지연 시간을 교체한다. 그 후 k개만큼의 지연 시간에 대한 평균과 표준 편차를 구한 후, 신뢰 구간 99%를 위해 평균 + 2.5 x 표준 편차로 임계 지연 시간을 새롭게 업데이트한다. 이를 통해 신호가 전달 될 때마다 그 신호의 지연 시간이 분포에 반영되어 임계 지연 시간이 유동적으로 변경 된다. 이러한 알고리즘은 실제 환경에서의 다양한 경우에 대비할 수 있다. 첫번째로 갑작스럽게 노이즈가 발생하여 적은 수의 지연 시간이 늘어나는 경우, 적은 수의 지연 시간은 평균과 표준 편차에 크게 영향을 주지 않으므로 이러한 노이즈는 무시된다. 두번째로 환경이 바뀌어 전달 지연 시간이 지속적으로 늘어나거나 줄어드는 경우, 바뀐 환경의 분포에 해당하는 신호가 지속적으로 들어오고 기존에 저장되어 있던 신호가 새로운 분포의 신호로 교체되기 때문에 그에 맞게 임계 지연 시간이 바뀌어 바뀐 환경에서도 정상적으로 작동할 수 있게 된다. 이 과정에서 처음 몇 개의 요청은 거부될 수 있으므로, 클라이언트 프로그램은 서버프로그램과 지속적으로 에코 메시지를 주고 받아 이 에코 메시지의 지연 시간을 반영하면 바뀐 환경에 보다 빠르게 적응하여 임계 지연 시간을 조정할 수 있으므로 환경이 바뀌었을 때 최초에 몇 개의 요청이 실패되는 경우를 방지할 수 있다.

3. 차량 문 개폐 시스템 구현



(그림 6) Intel Galileo Gen2 플랫폼(좌측)과 Raspberry Pi 플랫폼(우측)에 구현한 사용자 도메인 환경

제시된 시스템은 제조사, 판매자, 사용자 프로그램으로 나눠져 있다. 제조사, 판매자 프로그램은 윈도우10 환경에서 자바 언어를 사용한 데스크톱 애플리케이션으로 구현하였다. (그림 6)은 사용자 도메인을 구현한 환경을 나타낸다. 사용자 도메인은 클라이언트 프로그램과 서버 프로그램으로 나뉜다. 클라이언트 프로그램은 Raspberry Pi Model B+ 플랫폼(그림 6 우측)에서 실행되는 자바 프로그램으로, 관리자가 인가해준 차량 관리 권한을 바탕으로 차량 문 개폐를 요청한다. 서버 프로그램은 Intel Galileo gen2 플랫폼(그림 6 좌측)에서 실행되는 자바 프로그램으로, 클라이언트 프로그램으로부터 차량 문 개폐 요청을 받아서 요청이 유효한지를 타임스탬프 값과 임계 지연 시간을 기반으로 판단하고 차량 문 개폐 동작을 수행한다. 이때 차량 문 개폐가 올바르게 수행 되었는지를 확인하기 위해, LED를 이용해 차량 문 개폐가 성공 했을 경우, LED 불이 켜지도록 구현하였다.

<표 1> 100,000개의 차량 문 개폐 신호에 대해 임계 지연 시간 500ms를 기준으로 인증 정확도를 측정한 결과

	허용 신호	거부 신호	합계
퍼센티지(%)	99.993%	0.007%	100%
수(개)	99,993개	7개	100,000개
평균지연시간 (ms)	425.68ms	538.43ms	425.69ms

구현한 사용자 서버 프로그램과 클라이언트 프로그램을 이용하여, 실험실 환경에서 고정 임계 지연 시간을 사용했을 때의 차량 문 개폐 신호의 인증 정확도를 측정하였다. 총 100,000 개의 차량 문 개폐 요청 신호의 인증 정확도 측정을 수행한 결과는 <표 1>과 같다. 인증 성공과 실패의 기준을 정하기 위해, 사전에 미리 100,000 개의 차량 문 개폐 요청 신호의 평균 지연시간과 표준 편차를 구하였다. 평균 지연 시간은 약 425ms 이고, 표준편차는 약 30ms 이다. 요청 신호가 대략적으로 정규 분포를 따르므로, 신뢰도 99퍼센트 구간을 위한 임계 지연 시간 = 평균 표준 지연 시간 + (2.5 x 표준 편차) 이다. 이를 통해 임계 지연 시간을 구하면 임계 지연 시간 값은 500ms 이다. 이를 기준으로 또 다른 100,000개 신호의 정확도를 측정한 결과, 99.993%의 허용된 신호와, 0.007%의 거부된 신호가 측정되었다. 거부된 신호는 총 7개로, 각각 528ms, 502ms, 514ms, 528ms, 552ms, 571ms, 574ms 이었다. 실제로 이 신호들은 중계 공격을 실행 했을 때의 신호는 아니므로, 거짓 양성 반응에 해당한다. 따라서 인증 정확도는 99.993%라고 할 수 있다. 이를 통해 구현한 시스템의 인증 정확도가 약 99.99%에 달함을 확인하였다.

4. 결론

본 논문에서는 제조사 도메인부터 판매자 도메인, 관리자 도메인, 사용자 도메인 이르기 까지 서명과 암호화를 이용한 안전한 사용자 계정 생성 프로세스를 제안하고, 사용자 도메인의 차량 문 개폐 시스템을 임베디드 기기를 이용해 실제로 구현하여 인증 정확도를 측정하였다. 사용자 클라이언트 프로그램과 서버 프로그램간의 통신 지연 시간을 측정하여 임계 지연 시간 보다 클 경우, 차량과 사용자가 충분히 근접하지 않았다고 판단하여 차량 문 개폐를 허가 해주지 않는 지연 시간 기반 근접 여부를 측정을 하였다. 이를 통해 중계 공격 과정에서 필연적으로 발생하는 추가적인 지연 시간을 탐지하고 이를 기반으로 중계 공격을 막을 수 있는 차량 문 개폐 시스템을 제안하였다. 향후 연구를 통해, 본 논문에서 제시한 실제 환경에서의 유동성을 고려한 적응 임계 지연 시간에 대한 실험을 진행하여, 적응 임계 지연 시간의 실효성을 검증할 필요가 있다.

참고문헌

[1] Hancke, Gerhard P. "A practical relay attack on ISO 14443 proximity cards." Technical report, University of Cambridge Computer Laboratory 59 (2005): 382-385.

[2] Francillon, Aurélien, Boris Danev, and Srdjan Capkun. "Relay attacks on passive keyless entry and start systems in modern cars." Proceedings of the Network and Distributed System Security Symposium (NDSS). Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.

International Conference on. IEEE, 2016.

[3] Oman, Todd P., and Kevin J. Hawes. "Relay attack prevention for passive entry passive start (PEPS) vehicle security systems." U.S. Patent No. 8,930,045. 6 Jan. 2015.

[4] Turan, Meltem Sönmez, et al. "Sp 800-132. recommendation for password-based key derivation: Part 1: Storage applications." (2010).