Analisis Serangan Denial of Service pada Kunci Otomatis Berbasis Wifi

Rafi Saeful Rahman[1], Dr.Maman Abdurohman,S.T.,M.T.[2], Aji Gautama Putrada S,S.T.,M.T.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]rafisaefulr@students.telkomuniversity.ac.id, [2]abdurohman@telkomuniversity.ac.id,
[3]ajigps@telkomuniversity.ac.id

Abstrak

Pada makalah ini penulis mendemonstrasikan serangan *Denial of Service* (DOS) pada *Keyless Entry and Start* (KES) untuk mencegah terjadinya serangan *playback attack* pada KES. Di dalam sebuah mobil modern terpasang alat elektronik untuk meningkatkan keamanan dan kenyamanan pengguna. Secara tradisional untuk mengakses dan menghidupkan mobil terdapat kunci fisik, dengan memasukan kunci yang sesuai ke dalam pintu dan starter, pengguna dapat masuk dan menghidupkan mobil. Dalam satu dekade terakhir, terdapat penambahan pada sistem kunci berupa akses jarak jauh, yang mana pengguna akan mampu membuka mobil dari jarak jauh dengan menekan tombol pada *key fob*. Tetapi, untuk dapat menghidupkan mobil masih menggunakan kunci fisik. Belakangan ini perusahaan mobil telah memperkenalkan *Keyless Entry and Start* (KES) yang mampu mengakses dan menghidupkan mobil tanpa menggunakan kunci fisik asalkan kunci mobil dengan sistem KES tersebut berada dalam 'saku' pengemudi. Fitur ini sangat memudahkan disaat pengguna akan membuka kunci pintu dan menghidupkan mobil tidak perlu lagi menggunakan kunci fisik. Dalam penelitian ini, sistem keamanan pada KES dinyatakan rentan terhadap serangan *playback attack*. Pada serangan *Playback Attack*, penyerang menggunakan dua buah alat. Alat pertama ditempatkan berdekatan dengan kunci, alat kedua ditempatkan berdekatan dengan mobil. Kemudian penyerang akan mengirimkan sinyal melalui alat tersebut dari kunci asli ke mobil yang mengakibatkan mobil dapat dibuka dan dinyalakan meskipun kunci asli jauh dari mobil. Penyerangan tersebut disesuaikan dengan sekenario ketika kunci berada dalam saku pengemudi yang sedang berada di toko swalayan, dan mobil berada di parkiran. Penyerangan *Denial of Service* (DOS) akan dilakukan pada sistem KES. Penyerangan DOS ditujukan untuk membebani sistem KES agar tidak bisa berfungsi guna mencengah serangan *Playback Attack*.

Kata kunci : mobil modern, sistem kunci mobil, *keyless entry and start, denial of service, playback attack*

Abstract

In this paper we demonstrate Denial of Service (DOS) attack on Keyless Entry and Start (KES) to prevent playback attack. Modern cars embed electronic devices to improve driver safety and convenience. Traditionally, access and authorization have been achieved using physical key, where by inserting a correct key into the door and ignition, the user was able to enter and drive the car. In the last decade, this system has been augmented with remote access in which users are able to open their car remotely by pressing a button on their key fob. In these system, the authorization to drive was still using a phsycal key. Recently, car manufacturers have introduced Keyless Entry and Start (KES) system that allow users to open and start their car while having their car key in their 'pockets'. This feature is very convenient for the users since they don't have to use physical key. In this work, we analyze the security of KES system and show that system are vulnerable to playback attack. In playback attack, the attacker places one of his device in the proximity of the key, and the other device in the proximity of the car. The attacker than relay signal between the key and the car, enabling the car to be opened and started even if the key is far from the car. This corresponds to the scenario where the key is in the owner's pocket in the supermarket, and the car is at the supermarket parking lot. Denial of Service (DOS) attack will launched into KES system. DOS attack is intended to make KES system fail to provide normal service and prevent playback attack.

Keywords: modern car, car lock system, keyless entry and start, denial of service, playback attack