BioFIM: Multifactor Authentication for Defeating Vehicle Theft

Hasan Tahir and Ruhma Tahir

***Abstract*—A major problem today for car owners is that they are in constant fear of having their vehicles stolen from a common parking lot, from outside their home or the vehicle could be snatched from them while they are driving. In this paper a methodology for defeating car theft is proposed referred to as BioFIM- Biometric Flash Identification Module. Our proposed scheme fulfils both requirements of security as well as user convenience. The proposed BioFIM is a revolutionary idea for the car industry, by which a combination of fingerprints, portable flash drive and digital certificates can prevent car theft. The proposed scheme is designed to recognize its owner and will replace the common key. The features of the proposed BioFIM conclude that this particular scheme will be more resilient against car theft than the existing schemes in terms of security and user convenience.**

***Index Terms*—BioFIM (Biometric Flash Identification Module), Digital Certificate, Fingerprint, Multifactor Authentication.**

I. Introduction

According to statistics [1] a vehicle is stolen every 26 seconds in America alone. Until now over 700,000 vehicles are still not recovered. These vehicles are either roaming the streets, illegally exported or disassembled in chop shops. When a car thief has successfully stolen a vehicle his major focus is on getting the vehicle to a safe location where he is not distracted and he can disassemble the vehicle without any interference.

To drive away the vehicle, they need a key to enter the car. Current methods of preventing car theft include the use of an immobilizer key which has been proven effective against car theft but according to a report [2], there has been an evident increase in the number of vehicles being stolen due to key theft. Thieves have been able to steal a vehicle's key from the owner by burglary, robbery or taking without consent. This method of car theft makes the use of the immobilizer useless because after theft of the key the thief is able to drive away the vehicle.

Consequently, an authentication mechanism is needed that prevents the possibility of car theft in any case. There is need for a multifactor authentication mechanism that can be easily embedded into vehicles and prevents against all sorts of car theft. The drivers should be easily authenticated without having to carry additional mechanisms for authentication.

In this paper we propose a car theft prevention methodology BioFIM by using multifactor authentication. Section 2 describes what we mean by the employment of multifactor authentication in our proposed BioFIM. The building blocks of our proposed BioFIM are discussed in Section 3, with the details of its working and various factors which characterize it as a secure scheme. Section 4 throws light on the slight variations that could be made in BioFIM. The analysis of effectiveness of BioFIM is presented in section 5. The conclusion of the reserach is presented in section 6.

Manuscript received February 29, 2008.

H. T. Hasan Tahir is with the Computer Science and Engineering Department, Bahria Institute of Management and Computer Sciences, Shangrilla Road, E-8, Bahria University, Islamabad, Pakistan (phone: 0092-0333-5241987; fax: 0092-051-9257201; e-mail: hasanmailbox@yahoo.com).

R. T. Ruhma Tahir is with Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Lalkurti, Rawalpindi Cantt, Pakistan (e-mail: ruhma@mcs.edu.pk)

II. Multifactor Authentication

Multifactor authentication, is a system in which a user is required to provide multiple articles for authentication for example 'something the user has', 'something the user knows' and 'something a user is composed of'.

Multifactor authentication for vehicles can be done by providing a user with a unique key in combination with biometrics and vehicle specific data. If we combine biometrics with a portable memory device we would be able to provide a mechanism in which the chances of having an unauthorised person drive away a car will become significantly low. Mazda came up with a concept car named Sassou in 2005 [3]. One of the major features of the proposed vehicle is that it uses a common USB flash drive to program the car. Other car manufacturers have also considered a USB flash drive as a way of replacing the common key.

According to the US Patent 7006914 a portable memory device can be used in place of a key for the following purpose, as in [4]:

> *"A portable memory device used in substitution of an automobile key and interfaced with an automobile onboard computer and ignition system. The portable memory device contains data that, when read by the onboard computer, enables the ignition system."*

III. BioFIM Security Building Blocks

Conventional authentication methodologies are mostly key oriented. Drivers prefer to secure their vehicles with steering locks, remote alarms and immobilizer keys. To get enhanced security people prefer to use combination of security mechanisms such as steering locks coupled with remote control alarms or immobilizer keys. In these conventional mechanisms there is little user convenience and the chances of breach are still relatively very high. In our design, we aim to improve the security properties without increasing too

much cost. We construct a multifactor authentication scheme called BioFIM which prevents car theft by the combination of biometrics, vehicle specific certificates and USB 2.0. Our major objective in designing a new security module is to minimize cost-effect, while maintaining required levels of security along with user convenience.

A. Biometrics

Biometrics gives us a method of verifying a person on the basis of a biological factor. Biologically all humans are unique and different. A biometric system uses a human characteristic that's unique, universal, permanent and easily collectable by the system. Currently biometry techniques include facial recognition, voice recognition, retina recognition, iris recognition, handprint identification and fingerprint identification.

Many car manufacturers have already incorporated fingerprint readers into their vehicles to verify the driver. Perhaps the greatest advantage of using fingerprint verification system is that a person can never loose his fingerprint and the cost incurred in the deployment of fingerprint verification system is relatively less as compared to the other biometry techniques.

B. Vehicle Specific Certificates

Every vehicle will have its own digital certificate. These certificates will be slightly different from the conventional digital certificates used in digital communications. These certificates will be issued by the registration authority (RA) instead of a certification authority (CA). These certificates will contain numerous fields like the registration authorities' information, car owner's credentials, and information about the car (date of manufacture, make, model, engine type etc). Furthermore, the digital signature will be formed by taking the car owner's fingerprints and encrypting them with the private key of RA and appending with the certificate. The obtained certificate will be embedded into a special dedicated electronic module/ computer in the car from where the certificate can be accessed at a later time by only the RA. The electronic module into which the certificate is written should protect the certificate from being changed or erased by an unauthorized entity. Fig 1 shows the working of the proposed BioFIM model.

The greatest advantage of using such certificates will be that they will help in keeping track of vehicle records and provide a mechanism in which the police, RA or a custom control can check the vehicles and users credentials, by connecting the car's electronic module to their own system.

C. USB Flash Drive and User Credentials

A copy of this certificate will be written onto a specially designed USB flash drive which cannot be overwritten. This flash drive will be issued to the car owner and it will replace the conventional key mechanism used in cars. More than one flash drives will be issued to the owner to provide backup in case the owner looses a flash drive.

The RA's public key will also be provided within the flash drive. The public key may or may not be known to the general public because the electronic module will automatically pick the public key from the flash drive for decryption of the digital signature. Obviously the use of an incorrect public key will either lead to corrupt or wrong decrypted fingerprint.

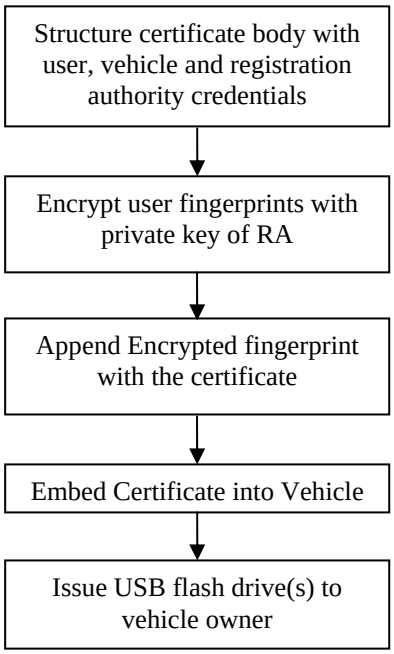

Figure 1. Certificate and Flash Drive Issuance Procedure

D. Running the Vehicle

In order to enter the vehicle the person will first pass through a fingerprint reader embedded in the door. To start the car the owner will plug the flash drive into a dedicated USB port found near or on the steering column. Then the user will place his thumb/finger on the fingerprint reader which will be located on the vehicles console.

On reading the fingerprint of the driver a decryption module will decrypt the digital signatures that are located in the inserted USB flash drive and the certificate that was embedded in the electronic module. Decryption of digital signatures will be done using the public key of the RA. The result of decryption will give us the fingerprint of the rightful owner. If the currently read fingerprint and all the decrypted fingerprints match this means the driver is the rightful owner, as in Fig 2.

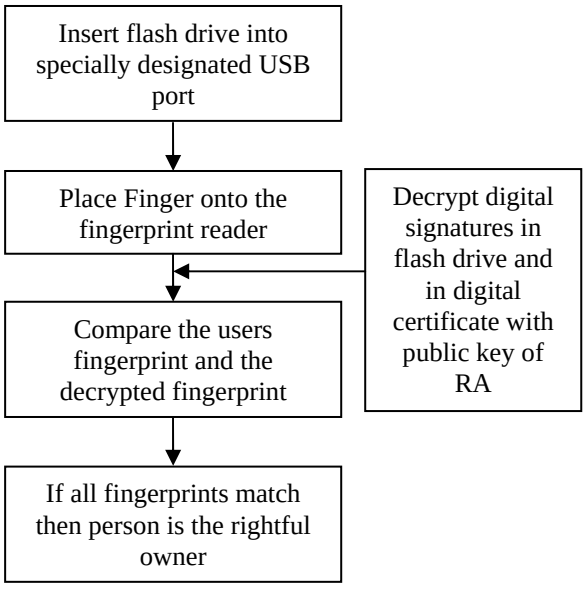

Figure 2. How the Vehicle Verifies the Current Driver

E. Verification by RA

If the RA wants to check the certificate in the USB or the vehicles module they can simply decrypt the digital signature of the certificate to obtain the users fingerprints. Then these prints will be verified with the prints found in the RA's record.

F. Stolen or Lost Flash Drive

If an owners USB flash drive is lost or stolen then the flash drive will not identify which car it belongs to, moreover the user of the flash drive will need the original owner's fingerprints to get the car started.

G. Multiple Car Drivers

Every vehicles certificate can be designed to accommodate the fingerprints of a large number of drivers. All the fingerprints will be encrypted with private key of the RA.

IV. Variations in the Scheme

A variation of BioFIM that can be implemented is, even if the fingerprint does not match the stored fingerprint but still the vehicle starts, then it runs at a severely restricted horsepower with disabled head and tail lights. The insurance company is automatically informed of the event, so that the vehicle can be tracked down. Kenworth Trucks formed a group with Heil Trailer International to produce a T-800 High-Tech Truck that uses a simple fingerprint reader [5]. This truck was designed to operate at extremely low horsepower if the fingerprint does not match the stored fingerprint, to further prevent theft the dispatch is also informed about the intrusion.

V. Analysis

A. Security Analysis

The strength of the solution lies in the fact that it combines biometrics with key cryptography. The fingerprints of a rightful owner of the vehicle are securely encrypted using the private key of the RA. This private key is only known to the RA which makes the scheme even more secure. In conventional techniques a person could produce a fake key to gain access to a vehicle but in case of the proposed scheme the chances of producing a fake USB flash drive with the correct fingerprints is fairly low.

B. Cost Analysis

The cost incurred in deployment of our proposed BioFIM will be relatively less as compared to other possible solutions which could possibly provide the same level of security. The cost of a fingerprint reader is very less as compared to the cost of other biometry techniques. Over the past few years USB drives have become very common and cheap so their deployment would also be very cost effective.

C. User Acceptance

We expect that our proposed BioFIM will have a very high acceptance rate because of the user convenience, while providing high levels of security. The user is not troubled by carrying around lots of authentication material for authentication, infact all he/she needs is a USB drive which might be smaller than a traditional car key.

VI. CONCLUSION

A fingerprint based entry system that is linked with a common USB flash drive will provide a mechanism which can lower car theft considerably. By using vehicle specific certificates the vehicles data and user credentials can be verified by the government authorities. The USB flash drive will be used to hold vehicle's information and the encrypted fingerprint of the owner. The proposed scheme provides the user with a key mechanism that is portable, electronically intelligent and it cannot be produced by car thieves or locksmiths, hence preventing all sorts of car theft.

References

[1] Auto Theft Statistics", http://www.rmiia.org/auto/auto_theft/statistics.htm.
[2] "Emerging Methods of Car theft – Theft of Keys." *London: Research, Development and Statistics Directorate.*
[3] G. Lee (2005), "Concept Car Uses USB to Program Vehicle and Replace Key".
[4] C.P. Cahoon, "U.S. Patent 7006914 Portable memory automobile ignition System".
[5] "Biometrics: Cars and Bikes with Fingerprint Sensors", http://perso.orange.fr/fingerchip/biometrics/types.