A New Approach in a Multifactor Authentication and Location-based Authorization

David Jaros, Petr Bednar, Kuchta Radek
Department of Microelectronics
Brno University of Technology, FEEC
Brno, Czech Republic
jarosd|kuchtar@feec.vutbr.cz, xbedna06@stud.feec.vutbr.cz

***Abstract* — This paper is focused on location-based authentication and authorization in a network environment. We propose a new approach, where the user's biometric credential and the user's location are used. A basic framework for the MALBA (Multifactor Authentication and Location-based Authorization) is defined in the article. We describe processes of initial binding, authentication and authorization. Finally, the MAD I (Multifactor Authentication Device) is introduced. The MAD I provides user's credentials for authentication and authorization processes. The user will get roles in the system dependent on his or her position.**

Keywords-location-based authentication; GPS; AES; multi-factor authentication; RBAC, embedded system

I. INTRODUCTION

Different contents and resources in the network environment require different security level. The security level is hard related to the user's authentication process. Protected services or resources that need higher security level adopt more effective authentication techniques. For example, a simply email client requires either login-password authentication (secret information). A user accessing to his or her bank account, where multifactor authentication technique is used, is a different case. The most often authentication techniques can be divided into three main groups. The first group is based on the knowledge of secret information, a password [1]. These authentication techniques are commonly used for authentication in the web services. The second group is formed by authentication techniques based on ownership of subject (token) that is unique in the system framework [2]. A token can be represented by a hardware key that is used for protection of computer program against illegal copying. The last group includes authentication techniques, which verify some of human user's biometric property such as fingerprint [3].

A piece of information about the user's current position is an additional factor that can be exploited in an authentication process, as refers [4]. The importance of the location-based authentication (LBA) is increasing especially for mobile users [5]. The advantage of LBA can be found in hospital sector as well. A doctor shouldn't handle with patient's privacy information out of hospitals. If is needed, he/she can define with cooperation with the administration desk the new safe area (his/her home). Also when the user wants to get access to his or her bank account, LBA can be used. The advantages of LBA are furthermore discussed in [5, 6].

The systems for access management are commonly called AAA systems (Authentication Authorization and Accounting) due to its processes [7]. The user's position information can be addressed into each of them. For a user's identity evaluating, rights dependent on his or her position can be assigned to the user's identity and finally a payment rate for services can dependent on his or her position.

The user's position is very sensitive information that can be abused in many cases. User's position can be also exploited for the position-targeted spam. For these reasons it should be operated very carefully with position information over whole its lifecycle. Position information should be anonymous as much as possible. The level of anonymity is dependent on required accuracy of position information. For instance, if the service requires position information for country determination, the position information shouldn't be interpreted in accuracy with a few meters.

In this article, we propose a new approach of mobile user authentication and authorization called MALBA that connects multifactor authentication and authorization. In our network framework we introduce embedded terminal MAD I (Multifactor Authentication Device) that performs user's fingerprint, user's position information and stores encryption keys.

The rest of the article is organized as follows. MALBA's application scenario, processes of the initial binding between MAD I and domain controller and authentication and authorization are described in the Section II. Next section introduces the MAD I. The final section is focused on conclusion and future work.

II. APPLICATION SCENARIO

We assumed the application scenario as shown in Figure 1. The user wants to get access to protected domain content as are resources, services clients. MAD I is connected to the user's terminal. The request for protected content from the user is redirected to domain controller which performs access management. The user is challenged for giving in its credentials. If the user has connected MAD I it provides position information and fingerprint. Methods for fingerprint processing generally product same hash for the same fingerprint, otherwise a fingerprint reader cannot be use in the identity verification. Position

 ISBN: 978-1-61208-125-0

information and fingerprint are encrypted by AES (Advantage Encryption System) [8]. The user adds its login and data are sent to a domain controller. The domain controller will solve user's authentication dependent on receipt credentials. If identity is verified, the user's roles in the domain are defined. For the system the RBAC (Role Based Access Control) is used [9].

An area management presents a database, which stores definition of user's areas. The areas are defined by two ways. A simpler way is to define one point and the distance from it (radius). Then we get a circle from where the user will get the access. The definition of net of triangles is more complex (leads to convex combination). This way is more difficult as for definition, storing and evaluating but gives us an advantage in definition area of any shape. Defined areas are stored within IDs and can be used by any users. The defined area can mean different roles (rights) for different users. The user can cooperate with the administration desk to define new area. A pairs area's ID - roles are stored in a user's profile in Active Directory. Dependent Appropriate areas are requested by domain controller from areas management. Domain controller contains an API for evaluating position information (if a user is or is not in evaluated position). The order in which area's IDs are stored in user's profiles defines areas priority. The last added ID in the list has the highest priority. This right solves the overlapping problem.

API in the domain controller evaluates mutual position between user's position and areas defined for its identity.

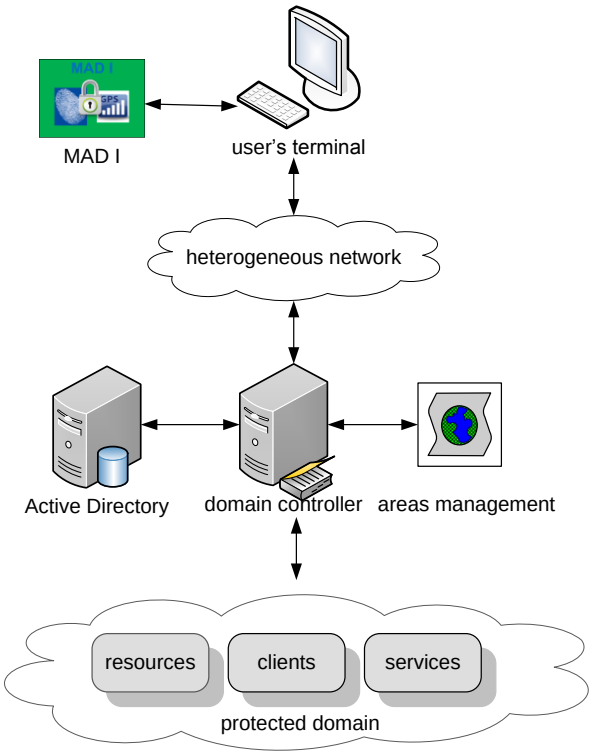

Figure 1. MALBA's application framework

A. *Initial binding*

Before the first user is authenticated mutual binding has to be done. Initial binding has to be executed at the system administration desk over local bus (MAD I is USB enabled). Binding process performs AES key exchange between MAD I and domain controller resp. Active Directory, where the key is stored during binding. A hash of user's fingerprint is also stored on the server side. This process can also cause MAD I can be assigned to exact user. Initial binding is described in Figure 2 in following steps.

1. At first, a secured channel should be established. This is done by Diffie-Hellmann key exchange [10]. Two unknown sides can derive the secret key. This technique is often used for exchange of symmetrical encryption key.
2. When the secured channel is established, domain controller generates encryption key for AES. Length of the key is 256 bytes.
3. The key is sent over the secured channel created in the first step.
4. The MAD I stores the key in secured memory after receipt.
5. The user is requested to swipe his or her finger on the fingerprint reader on the MAD I.
6. Hash of the user's fingerprint is sent to domain controller.
7. User's fingerprint hash is stored in the user's profile in the Active Directory.

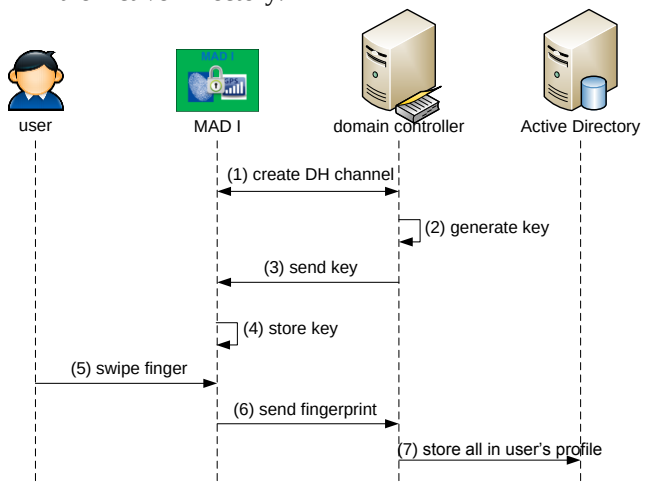

Figure 2. Initial binding

The areas are defined over GUI on the administration desk. The defined areas have to be stored for the current user in the area management and their IDs have to be stored with assigned roles in the Active Directory.

As written above we can define two kinds of areas. The first one is a circle defined by the center and its radius. To define general form we added the second type to the administration interface of area management that lies in the sequence formed by adding points. This feature exploits

 ISBN: 978-1-61208-125-0

math method of the smallest triangles and convex combination is used for evaluating.

B. *User's authentication*

When initial binding is done, both sides share the same encryption key and server side has stored the user's fingerprint hash. From this point server side is able to examine user's credentials as fingers. In next steps authentication and authorization processes are commonly described. We assume that the MAD I will be used in areas with free view on the sky. For indoor using, controlled areas should be covered by signal from signal repeater GPS. The situation is illustrated in Figure 3. The description starts after server side's request for credentials.

1. During the first part of the whole process user's credentials should be collected. Therefore the user swipes his or her finger.
2. The GPS (Global Position System) receiver gets position coordinates. The MAD I has to wait after power on for the position evaluating dependent on signal conditions.
3. The position *LOC* is encrypted by AES and user's finger print hash *UHFP* is used as key. The product of this step is cipher *EL*.
4. The second step of the encryption on the client side is provided by encryption cipher *EL* from the second point by symmetrical key *KEY*. The product is cipher *EAD*.
5. The encrypted credentials are sent to the user's terminal.
6. The user is requested to type his or her login.
7. The login with the user's credentials is sent to the domain controller.
8. The domain controller requests from the Active Directory needed data form user's that is related to received login. Data contains shared KEY, user's fingerprint hash and for user defined pairs (area ID – roles).
9. The domain controller receives requested data from the Active Directory.
10. The domain controller decrypts received cipher *EAD* by *KEY* from the active directory. The product of this step is *EL'*.
11. The domain controller tries to decrypt EL' by user's fingerprint hash CHFP from the Active Directory. If the result is an understandable position information, the user's identity is authenticated.
12. The domain controller sends a request to the area management, defining areas for the user.
13. The domain controller gets the IDs dependent on requested area from the areas management.
14. User's position is evaluated in relation to defined areas on the domain controller.
15. Dependent on the results from the previous step, the user has assigned roles for the current domain.

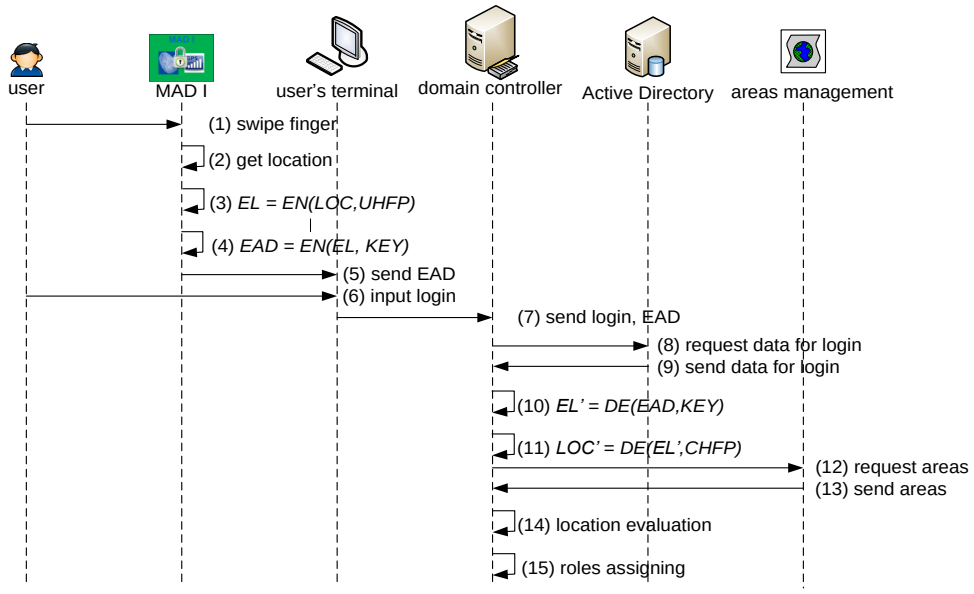

Figure 3. Authentication a authorization processes

III. THE MULTIFACTOR AUTHENTICATION DEVICE I

Multifactor authentication device MAD I was developed for the MALBA's framework.

The MAD I collects principally three authentication factors as ownership of certain device, fingerprint and user's position, where the user's position is used in the authorization as described in the second section.

The MAD I is connected to user's terminal via USB (Universal Serial Bus). The device is designed as a pocket

 ISBN: 978-1-61208-125-0

device. The block diagram of the MAD I is in Figure 4.

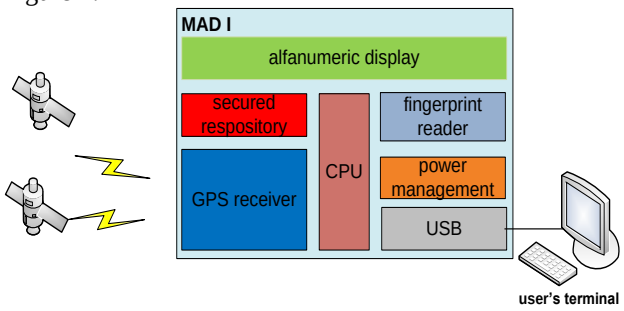

Figure 4. The MAD I block diagram

The position information is provided by the receiver GPS. The assembled GPS received is ready to Galileo for future use with European GNSS (Global Navigation Satellite System). As described above, the fingerprint reader is used for the user‘s authentication. For the security reasons the symmetrical encryption key is stored in the secured data repository. The secured data repository has special features that protect stored data against to unauthorized reading or writing. Alphanumeric display is assembled for communication between the user and MAD I.

The MAD I is a battery-powered pocket device. The power management contains circuits for adjustments power voltages for the other blocks and circuits for battery charging over USB.

IV. CONCLUSION AND FUTURE WORK

The importance and possible applications of the user’s position information in the access management is discussed in this article. We introduced the newly designed technique MALBA which is addressed for authentication and authorization of mobile user in the WLAN (Wireless Local Area Network) environment. We described the process of initial binding between device MAD I and domain controller. Next, the authentication and authorization processes are described. The device MAD I is described in the final section.

The hardware implementation of the MAD I is already done. The future work will be focused on software implementation of the MAD I. Setting up a test bed for testing proposed technique in real conditions has to be worked on also. We will test proposed technique in the ordinary network environment. The results from testing will be used as input data for next development and will be published.

ACKNOWLEDGEMENT

This research has been supported by the Czech Ministry of Education, Youth and Sports in the frame of MSM 0021630503 *MIKROSYN New Trends in Microelectronic Systems and Nanotechnologies* Research Project, partly supported by 2C08002 Research Project *KAAPS Research of Universal and Complex Authentication and Authorization for Fixed and Mobile Computer Networks* in the frame of the National Program of Research II, ARTEMIS JU in Project No. 100205 *Process Oriented Electronic Control Units for Electric Vehicles Developed on a multi-system real-time embedded platform*, by ENIAC JU in Project No. 120001 *Nanoelectronics for an Energy Efficient Electrical Car*, partly by the Czech Ministry of Industry and Trade in projects FR-TI1/057 *Automatic stocktaking system* and FR-TI1/058 *Intelligent house-open platform*.

REFERENCES

[1] H. Jiang, "Strong password authentication protocols," in *Distance Learning and Education (ICDLE), 2010 4th International Conference on*, 2010, pp. 50-52.

[2] H. K. Lu and A. Ali, "Communication Security between a Computer and a Hardware Token," in Systems, 2008. ICONS 08. Third International Conference on, 2008, pp. 220-225.

[3] E. Sano, et al., "Fingerprint Authentication Using Optical Characteristics in a Finger," in SICE-ICASE, 2006. International Joint Conference, 2006, pp. 1774-1777.

[4] E. Bertino, et al., "Location-Aware Authentication and Access Control - Concepts and Issues," in 2009 International Conference on Advanced Information Networking and Applications, ed, 2009, pp. 10-15.

[5] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, vol. 1996, pp. 12-16, 1996.

[6] G. Lenzini, *et al.*, "Trust-enhanced Security in Location-based Adaptive Authentication," *Electronic Notes in Theoretical Computer Science*, vol. 197, pp. 105-119, 2008.

[7] H. Rui, *et al.*, "A novel service-oriented AAA architecture," in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, 2003, pp. 2833-2837 vol.3.

[8] L. Chi-Feng, *et al.*, "Fast implementation of AES cryptographic algorithms in smart cards," in *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on*, 2003, pp. 573-579.

[9] M. L. Damiani, *et al.*, "GEO-RBAC: A spatially aware RBAC," *Acm Transactions on Information and System Security*, vol. 10, Feb 2007.

[10] Y. Eun-Jun and Y. Kee-Young, "An Efficient Diffie-Hellman-MAC Key Exchange Scheme," in *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on*, 2009, pp. 398-400.

 ISBN: 978-1-61208-125-0