The Space-Time Information in the Access Management

Jaroslav Kadlec, Radimír Vrba, David Jaroš, Radek Kuchta
Department of Microelectronics
FEEC, Brno University of Technology
Brno, Czech Republic
kadlecja | vrbar | jarosd | kuchtar@feec.vutbr.cz

***Abstract*—This paper deals with the possibility to employ the user's time and space position information in the access management. Using the time and space information as new factors for authentication process is discussed in this paper. We have also considered the issues of indoor localization and possible application scenarios where these two additional authentication factors can be applied. We have developed the Multi-Factor Authentication Device (MAD I) together with active infrastructure, which is required for indoor users' localization, to demonstrate the new main functions and advantages of adding time and space position to the user's authentication factors. The main advantage of the MAD I is that the device helps the AAA system verify the user's location in both main usages, i.e., indoor and outdoor environment.**

Keywords-location-based authentication; active infrastructure; wireless communication.

I. INTRODUCTION

Authentication and authorization are required almost everywhere in today's world. People must be identified when they download emails, read newspapers over the Internet, fill out forms for the government, access company private information, etc. When servers communicate with each other, they have to create trusted connection. Before a connection is created, it is necessary to identify the servers. There are different ways how to identify a user and a server.

The techniques that are used for user´s identity verification can be divided into three main groups along the subject of verification as refers [1].

- **A user knows something –** the user has to know private information, which is not known by anybody else. The password verification technique is one of the most common techniques in this group.
- **A user is somebody –** this group covers techniques that are related to human user authentication. The techniques verify biometric properties of a human´s body. The fingerprint reading technique can be mentioned here.
- **A user has something –** the user brings up a unique thing (token) as subject of credential. For example, the unique thing can be Radio Frequency Identification (RFID) transponder or a hardware key.

When a user or a server needs to authenticate a server, the most common way is using certificates. In this scenario, a trusted authority issues a certificate that is used for asymmetric cryptography.

Especially, the scenario with the user's credentials is sometimes insufficient and some extra information is required for many situations and systems. The information should be the user's certificate, biometric identification or current position.

The main topic of the paper is focused on the possibility of employing the user's space-time information in AAA (Authentication Authorization Accounting) systems [2]. We assume that the space-time information will be used especially for user's identity verification.

The sharp growth in information, technologies and especially information systems require monitored and effective access control. A user has to approve his identity at first. Based on this step, an access management will assign the rights for the user. An accounting system that will create and store records about the user's activities should also be a part of the system. For example, the records can be used as input information for future system development or for an audit. The above mentioned functions are provided by the systems that are commonly called AAA (Authentication Authorization Accounting) systems. The blocks of the main AAA system features are shown in Figure 1. A user is authenticated at first. In the next step rights are assigned to the user. The records are created during a whole session and stored in a database.

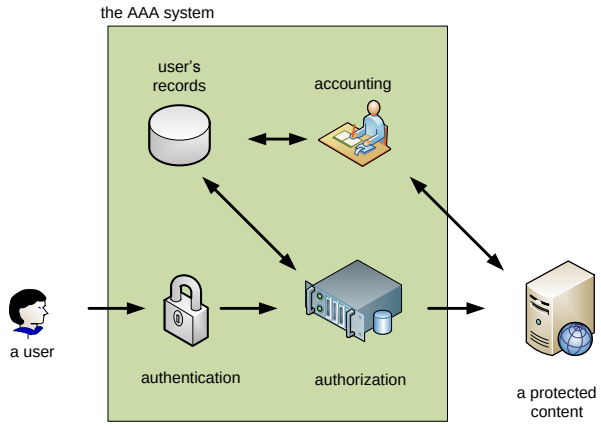

Figure 1. The main features of the AAA system

As a new factor of the user´s identity verification, his/her space-time information is discussed in this paper. That means "a user is on a known place in known time".

The rest of the paper is organized as follows: the space-time information introduction, the main aspects, and possible use in the AAA systems are described in the second section. The third section presents a possible application scenario.

 ISBN: 978-1-61208-183-0

The fourth section introduces an authentication technique with active infrastructure and with the Multi-Factor Authentication Device (MAD I).

II. THE SPACE-TIME INFORMATION

The AAA systems that could work with the space-time information can prove useful in the following fields.

For example, a doctor shouldn't manipulate a patient's private information outside the hospital area, as referred to in [3].

Another example can be found in the financial sector. The user's position verification should be a part of user authentication process before s/he gets access to the bank account.

The SSO principle (Single-Sign-On) [4] could also make use of the space-time information. The user does not need to perform authentication to various systems when they are accessed from approved places (from his/her home or office).

The position information can be interpreted relatively or absolutely [5]. The relative position is determined as proximity to the object the position of which is exactly known. The objects with known position are called anchor points. This interpretation is used in GSM (Global System for Mobile Communications: originally from Groupe Special Mobile). Second, the position information can be interpreted absolutely. The absolute position information utilizes the coordinates in two or three dimensions. This way is employed for example in GNSS (Global Navigation Satellite System) systems.

The space-time information can be assigned into all three main processes of the AAA system, as described in Figure 2. For the authentication the user's space-time information should be verified in conjunction with verification of other authentication factors. The process which performs verification of two or more factors is commonly called multi-factor authentication or strong authentication. Depending on the user's space-time information the user will get different access rights in the system. For example, when the user accesses from the office, s/he will get different rights than when doing so from a public internet café. The user's space-time information could also be used for choosing charging rate for services.

The space-time information is very sensitive private information. Generally, similar information is to be handled very carefully. As shown in [6], the user's space-time information could be abused in various ways.

The space-time information needs in the AAA systems are related especially to mobile users. If a user meets the space-time condition in the verification time, s/he will get access based on submitted credentials. The user has been verified and has access to the system, but he can change his position and move out from the approved area. This problem can be solved by periodically evaluating the space-time information.

The more suitable solution is described in [7]. Direction and speed of the user's movements is additional information used.

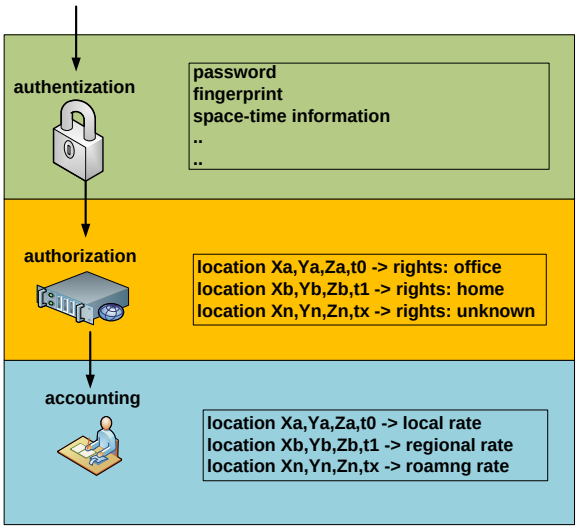

Figure 2. The space-time information in AAA

III. APPLICATION SCENARIO

We have adopted the application scenario as shown in Figure 3. The user wants to get access to the protected domain content (resources, services, etc.). The 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 requested to give in his/her credentials. If the user has connected MAD I, it provides the space-time information and fingerprint data. The methods for fingerprint processing in general provide the same hash for the same fingerprint, otherwise a fingerprint reader cannot be used in the identity verification. The position information and fingerprint are encrypted by AES (Advantage Encryption System) [8]. The user adds his login and the data are sent to a domain controller. The domain controller will settle the user's authentication depending on received credentials. If the identity is verified, the user's role in the domain is defined. The RBAC (Role Based Access Control) is used for the system [9].

An area management represents a database, which stores the definition of the user's areas. The areas are defined in two ways. A simpler way is to define one point and the distance from it (radius). Thus we get a circle from where the user will get the access. The definition of the net of triangles is more complex (leading to convex combination). This way brings along more difficulties in defining, storing and evaluating but gives us an advantage in the 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 a new area. The pairs of the area's ID - roles are stored in a user's profile in the Active Directory. Appropriate areas are requested by the domain controller from the management of areas. The domain controller contains API for evaluating the position information (if a user is or is not in an evaluated position). The order in which the area's IDs are stored in a user's

 ISBN: 978-1-61208-183-0

profiles defines the priority of the areas. The last added ID in the list has the highest priority. This right solves the overlapping problem.

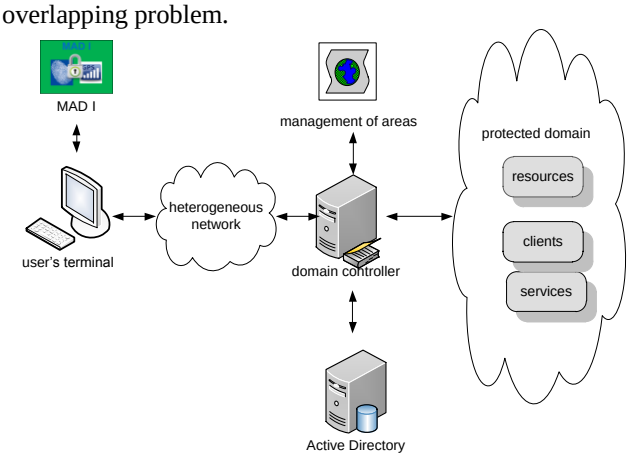

Figure 3. The application scenario with MAD I

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

IV. ACTIVE INFRASTRUCTURE AND MAD I

The Active Infrastructure (AI) is a technology background that is used in the two authentication techniques that are described in two subsequent sections. The key parts of AI are represented by an anchor point, a user's tag and an authenticator. The anchor point is located in position where the users want to be authenticated regarding their position. We assume that the position of the anchor point is exactly known to the authenticator. On the other hand, the user's tag is assigned to the particular user and only with difficulties is it related to its identity. The user's tag can be a part of the user's terminal or autonomy pocket device. The position of the user's tag is determined by proximity between the anchor point and the user's tag. When the user's tag can communicate with the anchor point, it means that it is nearby.

Figure 4 represents the active infrastructure key parts. The anchor point is in known position x_{AP}, y_{AP}, z_{AP}. If the user's tag is in its proximity, it can communicate with the anchor point which means that the position of the anchor point is similar to the position of the user's tag. The similarity between the positions is dependent on the range of transceivers. When the user claims that he is in a position nearby the anchor point, the authenticator asks the anchor point if an appropriate user's tag is in the communication range. It should be noted here that, for example, IQRF [10], Bluetooth [11], or similar wireless communication solutions can be used as wireless technologies.

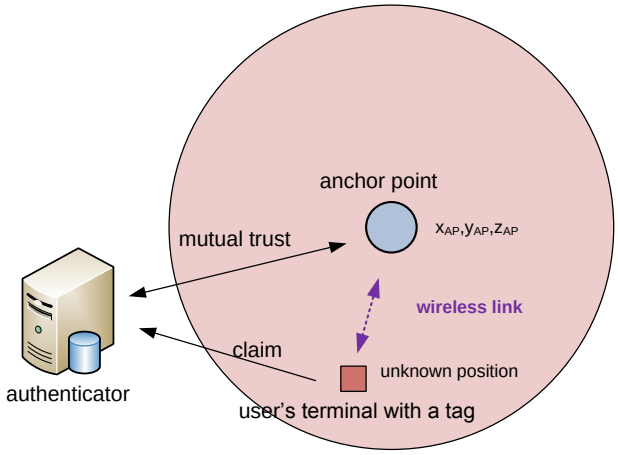

Figure 4. Principle of active infrastructure

Before the first user is authenticated, a 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 the domain controller or the Active Directory where the key is stored during the binding. The hash of the user's fingerprint is also stored on the server side. This process can also cause the assignment of MAD I to an exact user. The initial binding is described in the following steps.

- First, a secure channel should be established. This is done by Diffie-Hellmann key exchange [12]. Two unknown sides can derive the secret key. This technique is often used for the exchange of symmetrical encryption key.
- When the secured channel is established, the domain controller generates an encryption key for AES. The length of the key is 256 bytes.
- The key is sent via the secured channel created in the first step.
- The MAD I stores the key in secured memory after reception.
- The user is requested to swipe his finger on the fingerprint reader on the MAD I.
- The hash of the user's fingerprint is sent to the domain controller.
- The user's fingerprint hash is stored in the user's profile in the Active Directory.

The MAD I collects principally three authentication factors, i.e., the ownership of certain device, the fingerprint and the user's space-time information, where the user's position is used in the authentication process described.

The MAD I is connected to user's terminal via USB (Universal Serial Bus). The device is designed as a pocket device. The block diagram of the MAD I is shown in Figure 5.

 ISBN: 978-1-61208-183-0

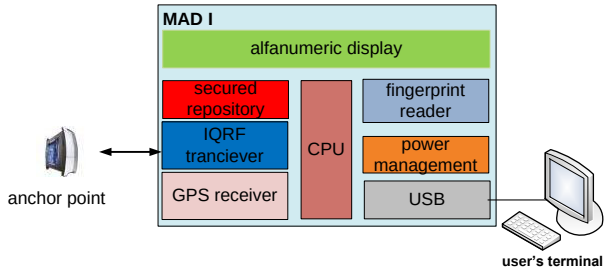

Figure 5. The MAD I block diagram

The position information is provided by the IQRF transceiver. The MAD I has already been assembled with GPS receiver for another way of position determination in other authentication techniques. The fingerprint reader is used for the user‘s authentication employing MAD I. For the security reasons the symmetrical encryption key is stored in the secure data repository. The secure data repository has special features that protect the stored data against 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 adjusting power voltages for the other blocks and circuits for battery charging via USB.

V. CONCLUSION AND FUTURE WORK

The paper has introduced quite a new direction in the access management which works with the user’s space-time information. We have enumerated the main aspects of possible applications. Further, we have described possible application scenario and a suitable solution while using the active infrastructure and the MAD I.

We have designed and developed a user’s Multi-Factor Authentication Device, prepared software for this device and started the testing phase of the project. The software for the MAD I device represents only one part of the required software. Another two software pieces had to be prepared. One is on the server side, which allows processing of the received user data and authentication factors and also integrates the position information to the Microsoft Active Directory.

The second part of the software has to be implemented to the user terminal. We are testing the available solutions. One is an extension of the Windows Credential provider. This has required installation to the client computer, an update of local policies and other administrative tasks. Second one can prove useful for public computers. In this case no installation is required. The software will only be executed and will communicate directly with the server and ensure user’s authentication. But this version has some limitations.

All the described methods are in the testing phase. The test results will be followed by other improvements. Also the MAD device is designed for testing purposes only and will be optimized and minimalized in the future.

ACKNOWLEDGMENT

This research has been supported by the ARTEMIS JU in Project No. 120228 AS Nanoelectronics for Mobile Ambient Assisted Living (AAL) Systems and partly by the Czech Ministry of Industry and Trade in project FR-FR-TI3/275 OPS An Open Platform for Smart Cities.

REFERENCES

[1] G. Lenzini, M. S. Bargh, and B. Hulsebosch, "Trust-enhanced Security in Location-based Adaptive Authentication," Electronic Notes in Theoretical Computer Science, vol. 197, pp. 105-119, 2008.

[2] R. He, M. Yuan, J. Hu, H. Zhang, Z. Kan, and J. Ma, "A novel service-oriented AAA architecture," Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on , vol.3, no., pp. 2833- 2837 vol.3, 7-10 Sept. 2003

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

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

[5] I. Ray and M. Kumar, "Towards a location-based mandatory access control model," Computers & Security, vol. 25, pp. 36-44, Feb 2006.

[6] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," Computer, vol. 36, pp. 135-137, Dec 2003.

[7] P. S. Tikamdas and A. E. Nahas, "Direction-based proximity detection algorithm for location-based services," in Wireless and Optical Communications Networks, 2009. WOCN '09. IFIP International Conference on, 2009, pp. 1-5.

[8] Ch. Lu, Y. Kao, H. Chiang, and Ch. Yang, "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] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: A spatially aware RBAC," Acm Transactions on Information and System Security, vol. 10, Feb 2007, pp. 1-39.

[10] MICRORISC. IQRF - wireless technology. <retrieved: 12, 2011> Available: www.iqrf.org

[11] B. SIG, Bluetooth homepage. <retrieved: 12, 2011> Available: www.bluetooth.com

[12] 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: 978-1-61208-183-0