The Location-based Authentication with The Active Infrastructure

David Jaros, Radek Kuchta, Radimir Vrba
Department of Microelectronics
FEEC, Brno University of Technology
Brno, Czech Republic
jarosd|kuchtar|vrbar@feec.vutbr.cz

Abstract - **The paper introduces location-based authentication techniques that are especially addressed to use in buildings and the environment, which is not covered by GPS signal (Global Position System). An active infrastructure is used as a source of position information. Two techniques are proposed. The first technique performs a remote user's authentication where the user's terminal broadcasts identity message. The active infrastructure evaluates user's position and informs an authenticator. The other proposed technique performs local user's authentication. The authentication process is launched on the user's terminal. The user's terminal collects information from its actual neighborhood and evaluates position information.**

Keywords - Location-based authentication, active infrastructures, local authentication, remote authentication

I. INTRODUCTION

The location-based authentication is a quite new direction in the access management. The direction gains in importance nowadays due to mobile devices coming to wireless network environment. The advantages and a possible application scenario is discussed in [1, 2].

The user's position information is required for access management systems more and more often. The user should bring up information about his/her position with the other credentials when he/she attempts to get access to protected service or content. For example, the user's right in the private company network can be assigned depending on his/her position. The access management system can make decision about the result of user's authentication or can assign set of rights depending on the user's position. The access management system is generally called AAA system (Authentication, Authorization and Accounting) regarding the three main processes covered in [3]. The user's position information could be processed mainly in the authentication and authorization. The authentication techniques that use user's position information are called location-based authentication.

In this paper, we propose two techniques. The first of them is remote authentication. The user accesses to remote network resources in this case and sends his/her credentials over the network. The authentication process proofs brought up credentials on the remote machine (server).

On the other hand, the local authentication is launched on the user's terminal; the user brings up credentials locally. This case is useful when the protected content or services are stored on user's terminal. The other possible application scenario can be found in authentication during logon to laptop operating system.

We can divide location-based authentication techniques depending on the source of position information into two main groups. The position information can be sourced from the user's terminal (for example GPS enabled) in the first group. The second group covers techniques where the user's position is evaluated by infrastructure (for example GSM network).

We introduce authentication techniques in which the position information is sourced from the infrastructure. The first technique is a remote type and the second one is a local type, as classification above refers.

The rest of this paper is organized as follows. The second section describes technology infrastructure that is used in the next two proposals. The third section introduces a new propose of the location-based authentication that is based on the active infrastructure and solves the remote authentication. The fourth section deals with our second proposal of the location-based authentication techniques. The second proposal is designed especially for local authentication in the user's terminal.

II. ACTIVE INFRASTRUCTURE

The active infrastructure (AI) is a technology background that is used in the two authentication techniques that are described in the next two sections. The key parts of AI are an anchor point, a user's tag and an authenticator. The anchor point is located somewhere from where some of the users want to be authenticated regarding to his/her position. We assume that the position of anchor point is exactly known for the authenticator. On the other hand, the user's tag is assigned to the particular user and it is hard related with his/her identity. User's tag can be a part of user's terminal or an autonomy pocket device. The position of user's tag is proclaimed in terms of proximity between the anchor point and the user's tag. When the user's tag can communicate with the anchor point it means that is nearby.

Figure 1 presents AI's key parts. The anchor point is on known position x_{AP}, y_{AP}, z_{AP}. If the user's tag is in neighborhood it can communicate with anchor point and it means that anchor point's position is similar to the position of user's tag. The similarity between the positions is dependent on the range of transceivers. When the user claims that he/she is on position nearby the anchor point, the

 ISBN: 978-1-61208-124-3

authenticator asks the anchor point if an appropriate user's tag is in the neighborhood. Here should be noted, that for example IQRF [4], Bluetooth [5] or something similar can be used as wireless technologies.

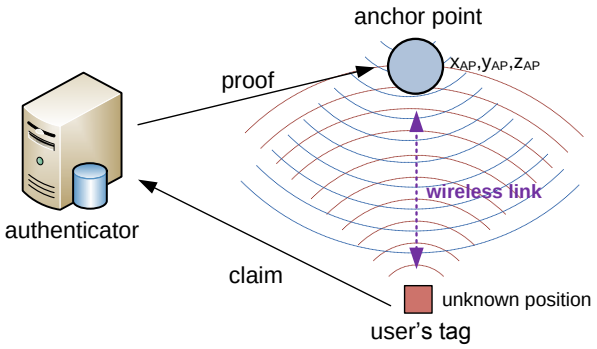

Figure 1. Principle of an active infrastructure

The relationship between the anchor points and the authenticator should be mutually trusted. We propose the use of symmetrical cryptographic system AES (Advanced Encryption System) that is described in [6]. The trusted relationship between communicating parts has to be established before the first use. An initial binding process covers key generation and its exchange. This process has to be granted by system administrator because it is crucial for system security. The binding process between the anchor point and the authenticator is described as follows.

1. First, a secured channel between both sides has to be established. This is provided by the Diffie-Hellmann's principle[7].
2. The authenticator generates AES's key that will be used in the future whenever the authenticator will communicate with this anchor point.
3. The generated key is sent through the secured channel to the anchor point.

The above described AI can vary depending on authentication technique in which it is used.

III. REMOTE AUTHENTICATION

We introduce remote location-based authentication technique with AI in this section.

A possible application scenario for remote location-based authentication is in figure 2. In this scenario user's authentication is processed and evaluated dependent on his/her position. The technique is provided by two independent processes. The first one is user's tag localization; this process is described as follows.

The user's tag is recognized by the anchor point as soon as it is in anchor point's range (A1). The anchor point informs AAA system about this event (A2).The AAA system creates a record in database (A3). Each record contains time, user's identification and anchor point's identification.

The second process is authentication that is initiated by user's requesting of the protected content. The whole process is described below.

1. User's request is redirected to AAA systems that provide access management.
2. AAA system will request credentials from user A.
3. User A will replay with his/her credentials.
4. Part of user's credentials is claimed user's position. The AAA system will query if it is the user who is currently authenticated in claimed position.
5. The AAA system receives answer from the database. When the user is on correct position and his/her position was proved, position condition has been fulfilled.
6. AAA system will inform server with protected content and user's terminal when each of brought up credentials are proved.
7. Access to protected content can be established after authentication and authorization processes are done and when they are correct.

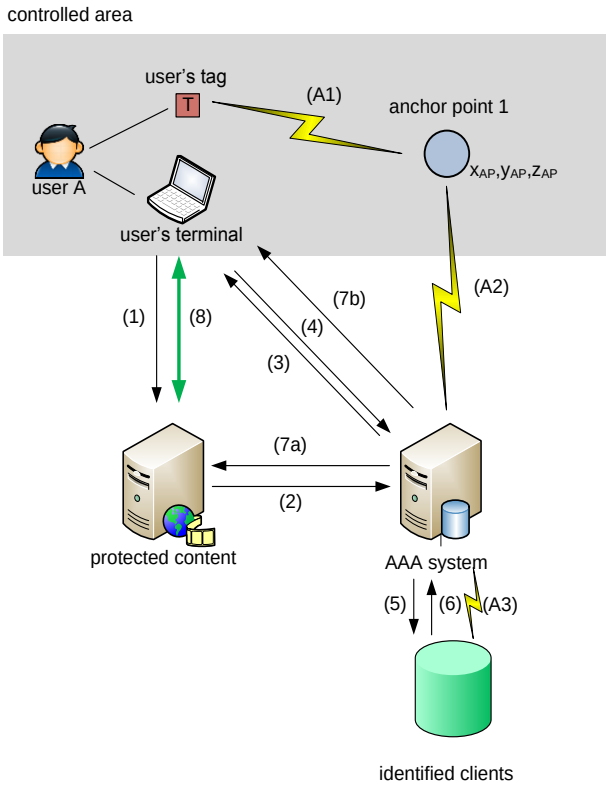

Figure 2. The remote location-based authentication schematic

The remote authentication can be adopted especially to protect sensitive information in private company network. The user has to be in his/her office when he/she wants to work with protected content. The position condition should be periodically tested to prevent user's moving out of

controlled area (out of the office). When a user moves out of controlled area, he/she lose access to protected content. Therefore a time period of re-authentication should be dependent on target application where is technique used.

IV. LOCAL AUTHENTICATION

The location-based technique for local authentication is described in this section. The technique is namely addressed to enhance login process in laptop operating system.

The main difference in comparison to remote authentication is the situation of the authenticator. The authenticator is a part of the user's terminal in this technique. The authenticator has to store a table with anchor point's positions and their encryptions keys, as well as it is in the remote authentication. Initial bonding between anchor points has to be done before the first use, too. In this case the user's tag is a part of authenticator and it can be used by different users. The authentication technique is described in Figure 3. The whole process can be depicted as follows.

When the user tries to log on his/her terminal, the user's tag is activated and it surveys its neighborhood. All available anchor points are captured. The user inputs the identification and other credentials if required. In regard to user's profile, there are processed authentication and assigned right in the authorization.

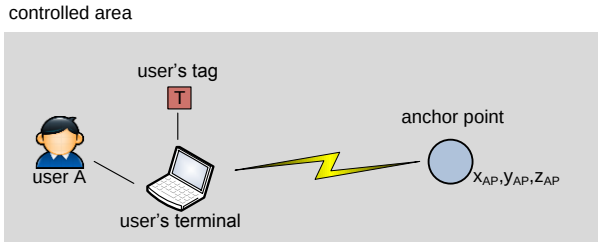

Figure 3. The local location-based authentication

The authentication technique shortly depicted above, could be suitable to assure that data stored on user's terminal will be viewed just in the right place.

V. CONCLUSION

The location-based authentication is a quickly developing field in the access management due to enhancement of mobile devices that are coming into the network environment. We can divide the above mentioned techniques into two basic groups dependent on the source of position information.

The active infrastructure is introduced in the second section. The active infrastructure provides position information of the authenticating user. The key parts of the active infrastructure are the anchor points and user's tags.

The main goal of the article is a proposal of the location-based authentication techniques that are usable in the environment where GPS signal is not available.

In the third section there is an application scenario of the active infrastructure being described. In this scenario the authentication process runs on a remote machine as it is frequent in the network environment.

The forth section introduced the other proposed technique that is namely addressed to local authentication on user's terminal. In this case an authentication's entity is part of the user's terminal.

The authentication techniques were theoretically proposed till now. The future work will be focused on implementation of the proposed techniques. The active infrastructure test bed should be assembled at first.

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

[2] Karaoguz and Jeyhan, "Location-based authentication of wireless terminal," US Patent, 2011.

[3] 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.

[4] Microrisc. (2011, 30-01). *IQRF homepage*. Available: www.iqrf.org

[5] B. SIG. (2011, 30-01). *Bluetooth homepage*. Available: www.bluetooth.com

[6] 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.

[7] 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: 978-1-61208-124-3