Multifactor Authentication Device

Jaroslav Kadlec, Radimir Vrba, Radek Kuchta
Faculty of Electrical Engineering and Communication Brno University of Technology
Brno, Czech Republic
kadlecja | vrbar | kuchtar@feec.vutbr.cz

***Abstract*— This paper describes a Multifactor authentication device, the main features of the device and implementation to the Microsoft Windows Credential Provider. The newest, more robust and more secure solutions for user's or system's authentication brings new challenges and requests to design completely new, advanced and highly trustworthy authentication devices. Nowadays one or two factor authentication can be in some cases too risky and vulnerable for security attacks. Therefore more authentication factors are required to increase authentication process security and minimize possible identity forge. Due to this reason a new authentication device, extended authentication process by another two factors, was developed and proposed in this paper.**

***Keywords*-** Multifactor authentication; authentication device; credential provider**.**

I. INTRODUCTION

Authentication and authorization are asked almost everywhere in the today's world. People must be identified when they download emails, read newspaper over the Internet, fill out forms for the government, access company private information, etc. When servers communicate to each other, they have to create trusted connection. Before the connection is created, it is necessary to identify servers. There are different ways how to identify a user and a server. For the user authentication some private credentials are usually required. In many cases users are using their unique identification number or username, and password. If one of these values is wrong, a new enter is required. If more than selected number of attempts has been done, user's account is locked.

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

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

This paper describes a new authentication device that allows determining of user position by GPS or wireless communication network, using PIN and fingerprint to authenticate a user and using user's certificate to sing these credentials before sending to an authentication server.

The paper also describes a new possibility of using position data as one of the authentication information. When an information system has information about authenticated person's position, it can change access rights or show only part of accessible data according to predefined access rules.

The first part of the paper describes the main aspects of current user position information using. Next section is a description of basic cryptographic methods used in user authentication process. Following section describes a new Multifactor Authentication Device (MAD) and the main parts of this device. Next sections describe Microsoft Windows Credential Provider and authentication process with connected Multifactor Authentication Device.

II. THE MAIN ASPECTS OF POSITION INFORMATION

Nowadays, many papers discuss using of user's location as a new factor of authentication process. Location-based authentication can be useful in many cases. The advantages of location-based authentication are presented in [1, 2]. One of the possible places for location-based authentication usage can be hospital sector. A doctor shouldn't handle with patients' privacy information out of hospital's border. Another example of location-based authentication we can find in the financial branch. If a user (account owner) would like to operate on his account, it should prove his location at first. If the user is at home or in a bank office, he will get access. If he is out of acceptable locations, he won't get the access to his bank account.

When the user's position is coming into the authentication process some aspects have to be taken into account.

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. The way how to achieve user's privacy protection is presented in [3]. 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.

The second aspect of position-based authentication is user's mobility. In the model situation, a user is authenticated upon its actual position (time t_0). From now the user has granted access, but the user is moving and the position condition can be disturbed (time t_1). The situation is illustrated in Fig. 1.

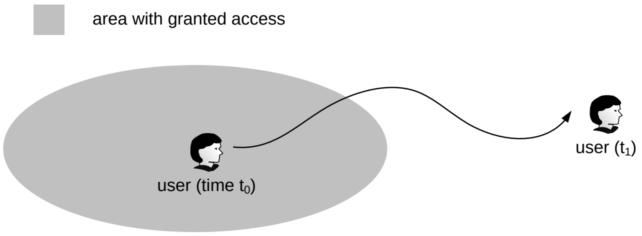

Fig. 1. Position condition collision

The way how to solve this problem is to re-authenticate the user's position periodically. This way is unusable for huge systems for large network resources requirements. Another way is depicted in [4]. Speed and direction of movements are used as additional information.

III. Basics of cryptographical background

The cryptography methods are very helpful and irreplaceable tools in authentication techniques. In Fig. 2 are listed, the main principles of cryptography systems that can be used in authentication techniques.

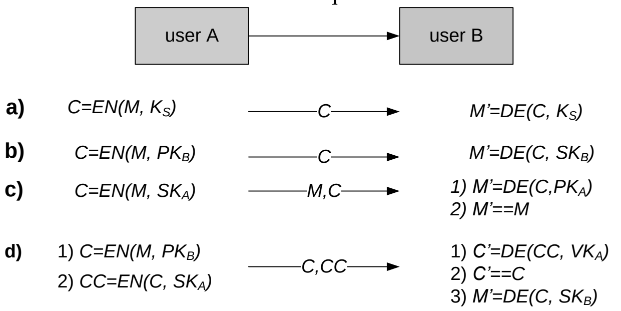
user A
user B
a) C=EN(M, KS) C M'=DE(C, KS)
b) C=EN(M, PKB) C M'=DE(C, SKB)
c) C=EN(M, SKA) M,C 1) M'=DE(C,PKA) 2) M'==M
d) 1) C=EN(M, PKB) 2) CC=EN(C, SKA) C,CC 1) C'=DE(CC, VKA) 2) C'==C 3) M'=DE(C, SKB)

Fig. 2. Basic cryptographycal principles

In Fig. 2 a) there is the principle of symmetrical cryptography system. Message *M* is encrypted by function *EN* and key K_S to cryptogram *C*. After reception *C* is decrypted by decryption function *DE* and same key K_S. The group of symmetrical cryptosystem represents AES (Advantage Encryption System) [5].

In asymmetrical cryptography systems two keys belong to everyone's entity. The first one is public key, known to each entity of the system, the other key is private and its *id* is known only for the appropriate entity. A message can be encrypted by any key (public or private), but for decryption the other key has to be used. In other words, a message encrypted by public key has to be decrypted by private key, and vice versa. Asymmetrical cryptosystem performs two basic functions. Confidentiality of message is performed when the message is encrypted on the sender's side by the recipient's public key PK_B and decrypted by private key SK_B on the recipient's side, Fig. 2 b). If the message is encrypted by sender's private key SK_A, the other side can prove sender's identity when decrypted by public key of the sender PK_A see Fig. 2 c). So, when we encrypt by private key we perform authenticity of the message, respectively encrypting by public key means confidentiality of the message. When we need authenticated confidential message we have to do every operation two times, encryption and decryption, as shown in Fig. 2 d).

The above described principles are used in the proposed techniques for mutual authentication between authentication terminal and AAA server (authenticator). Especially, the principle of Fig. 2 c) is used in newly designed techniques. To prove the origin of a message (authenticity) it has to consist of two parts. The first part is a plain text of a message, the other part is a cryptogram created by encrypting with sender's secret key. On the recipient's side there is a cryptogram decrypted by sender's public key.

Mutual authentication preserves system form third side's attack as depicted in the Fig. 3.

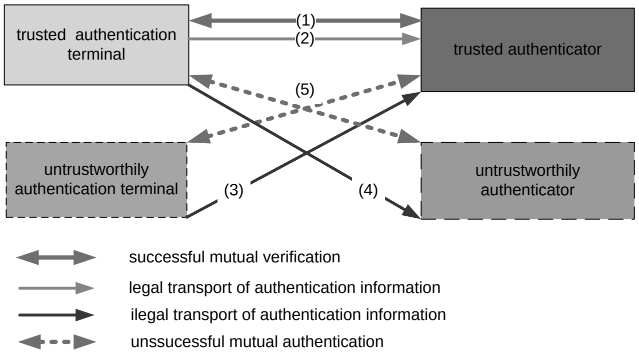
trusted authentication terminal
trusted authenticator
untrustworthily authentication terminal
untrustworthily authenticator
(1)
(2)
(3)
(4)
(5)
successful mutual verification
legal transport of authentication information
ilegal transport of authentication information
unssucessful mutual authentication

Fig. 3. Possible attacks to the authentication systems

Messages should be sent just between trusted pair (paths 1 and 2 from Fig. 3) (authentication terminal and authenticator – part of the server AAA).

Third side's device can emulate each device in the system, but we strongly rely on elimination of other possibilities as are depicted in Fig. 3.

IV. Wireless networks and their possibilities for position determination

When position of a subject in the space is needed to know three basic conditions have to be fulfilled. First, the space where the subject is found should be described. The most often coordinates are used to describe of the space [6]. Secondly, enough of anchor points with known position have to be had. And finally, distance between the subject and anchor points have to be found. Number of used anchor points depends on dimension of the space [7]. Example for two dimensional systems is depicted in Fig. 4.

General equation used for position determination is

$$(x-m)^2+(y-n)^2=r^2, \qquad (1)$$

where *m* and *n* are coordinates of the center of a circle (position of an anchor point), *x* and *y* are coordinates of points on the circle (possible position of the subject) and *r* is radius of the circle (distance between the anchor point and the subject). Then we can get equation system for getting position of our subject [8]

$$\begin{array}{l} (x-6)^2+(y-14)^2 = 5{,}83^2 \\ (x-7)^2+(y-7)^2 = 5{,}65^2 \\ \underline{(x-17)^2+(y-11)^2 = 6^2} \\ x=11;\ y=11 \end{array} \qquad (2)$$

.

When previous equation system is solved, coordinates of position of the subject will be gotten (for our example 11,11).

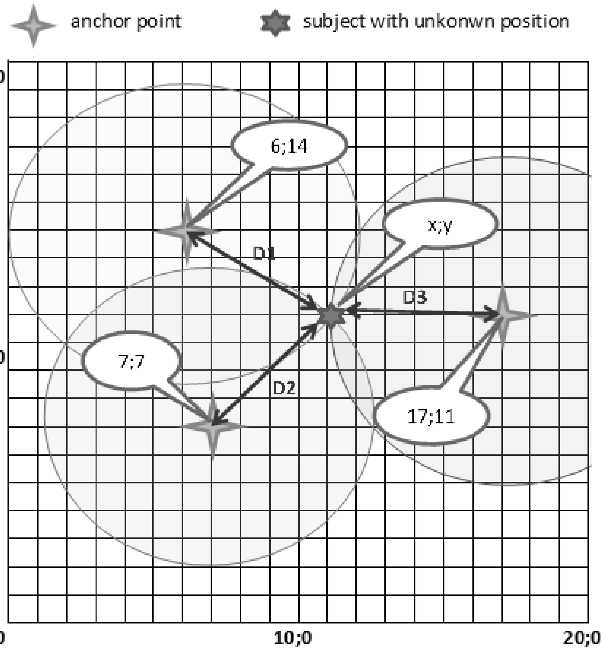

Fig. 4. Position determination with three wireless connection access points

When we use wireless communication network to determine current position, we use the same equation. In many cases it is not important to know exact position. If we would like to know that user is in corporate building, it is enough that he is in range of corporate wireless network or specific wireless transmitter.

V. Multifactor authentication device

For described methods of position determination some user device is needed.

Block diagram of the first generation of the user authentication device connected to the user terminal is shown in Fig. 5. User is using user terminal to connect to the authentication server in this scenario. This terminal is interconnected with the user authentication device via USB data bus. The core of the multifactor authentication device (MAD) is low powered central processor unit. The device contains secured data repository (SDR), where user's credentials are stored.

SDR is also a place, where user's certificate is stored. Each data, that are send to Authentication server are signed out by the user certificate.

SDR also stores trusted server certificates, or in the other scenario, the certificate of a trusted certification authority that issued server certificate. Whole device sends credentials only to the server, with valid and trusted certificate.

The third certificate stored in SDR is a device certificate. This certificate has to be valid and issued by certification authority that is trusted by authentication server.

Server certificate and device certificate are used to authenticate server and device together and to create secured communication channel.

Before data stored in SDR are accessed, the user has to open access to it by fingerprint login through fingerprint biometrics to PIN authentication.

The authentication device is connected to the user terminal with appropriate software that allows interconnection between the user authentication device and the authentication server, over the USB.

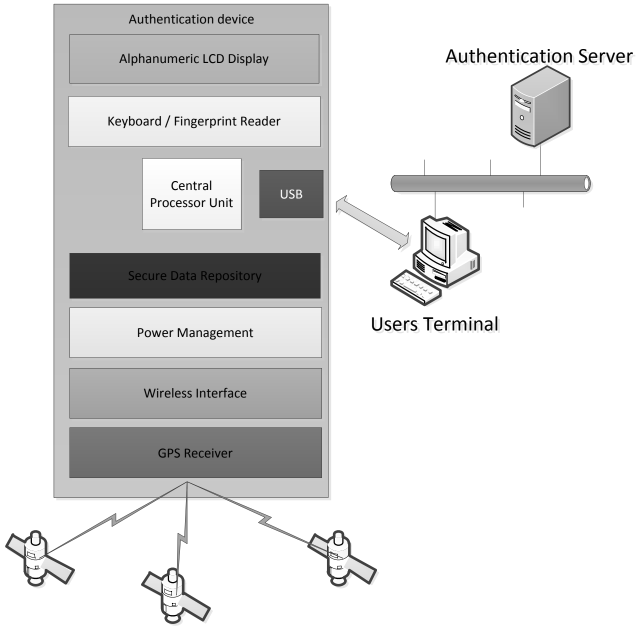

Fig. 5. Block structure of the user authentication device

If user is using standard computer without installed software or public computer, the authentication device also contains alphanumeric display where authentication instructions are shown. Thus, web access can be used for the user's authentication.

Current position of the device is determined by integrated GPS receiver. Current position is periodically stored to the internal memory with time stamp. When authentication process requires the device position and device is out of GPS signal, stored position with time stamp is used.

Different wireless interfaces are available on MAD to determine current position with company wireless network. There two main implementation. The first one is using WiFi and connection to wireless access points. The second one is using proprietary wireless communication platform IQRF. Principe of position determination is always the same how is described above.

VI. WINDOWS LOGON IMPLEMENTATION

Authentication protocols are implemented in Windows by security service providers. Windows Vista introduces a new authentication package called the Credential Security Service Provider, or CredSSP, that provides a single sign-on (SSO) user experience when starting a new Terminal Services session. CredSSP enables applications to delegate users' credentials from the client computer (by using the client-side security service provider) to the target server (through the server-side security service provider) based on client policies [9].

Credential providers [9] are in-process COM objects that are used to collect credentials in Windows Vista and run in local system context. In summary, the logon UI provides interactive UI rendering, Winlogon provides interactive logon infrastructure, and credential providers help gather and process credentials.

After all providers have enumerated their tiles, the logon UI displays them to a user. The user interacts with a tile to supply his or her credentials. The logon UI submits these credentials for authentication. Combined with supporting hardware, credential providers can extend the Microsoft Windows operating system to enable users to logon through biometric (fingerprint, retinal, or voice recognition), password, PIN, smart card certificate, or any custom authentication package a third-party developer wants to create.

Credential providers are not enforcement mechanisms. They are used to gather and serialize credentials. The LSA and authentication packages enforce security [12, 13, 14, 15].

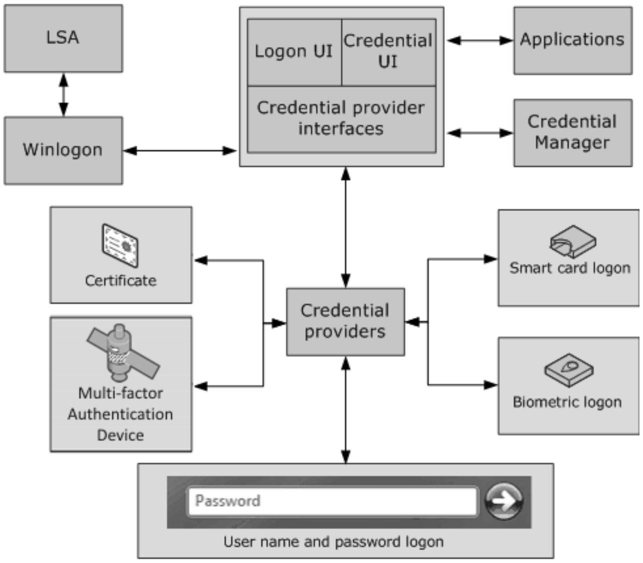

Fig. 6. Windows Vista hybrid credential provider architecture with integrated MAD CredSPP [10]

Credential providers are registered on a Windows Vista computer and are responsible for:

- Describing the credential information required for authentication.
- Handling communication and logic with external authentication authorities.
- Packaging credentials for interactive and network logon.

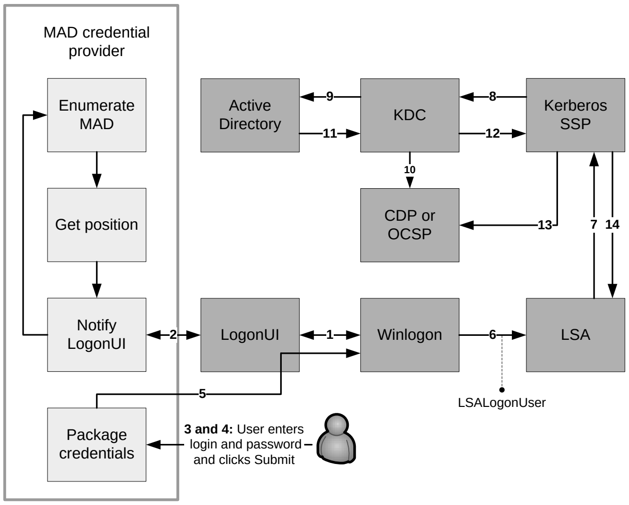

Fig. 7. Modified logon flow [10] for MAD authentication process

The hybrid credential provider architecture is shown in Fig. 6. The hybrid credential provider API does not design UI (User Interface) but describes which controls need to be rendered to windows logon screen. The hybrid credential provider interfaces with the Windows Smart Card API or Biometric API both directly and indirectly. The direct interface is via public routines, which allow the detection of connected biometrics or smartcard devices or even detection of inserted card. The indirect interface is via the custom APIs specific for each connected devices, which allow the credential provider to read a user credential directly from the device. The MAD credential provider uses own MAD API for low-level communication. Obtained user's credential from MAD through MAD API are combined with password from logon UI and sent to credential provider interface.

VII. AUTHENTICATION PROCESS

Authentication process with connected MAD is a combination of standard Windows logon process with custom scripts executed by the Active Directory (AD) user's policies [11]. Flow sequence of logon process within Multifactor Authentication Device (see Fig. 7):

1. Winlogon requests the logon UI credential information. Asynchronously, our multifactor authentication resource manager starts. The multifactor authentication credential provider:
   a. Gets a list of multifactor authentication devices (uses our MAD API).
   b. Get position information from connected multifactor authentication devices, the MAD credential provider copies it into a temporary secure cache on the terminal.
   c. Notifies the logon UI that new credentials exist.

2. The logon UI requests the new credentials from the MAD credential provider. As a response, the MAD credential provider provides to the logon UI actual position information. The user selects a multifactor authentication device logon title, and Windows displays a logon dialog box.
3. The user enters his login and password and clicks Go button.
4. The credential provider that resides in the LogonUI process (system) collects login, password and position. As part of packaging credentials in the MAD credential provider, the data is packaged in a KERB_INTERACTIVE_LOGON structure. The main contents of the KERB_INTERACTIVE_LOGON structure are User Name, Domain Name and Password.
5. The credential provider now wraps the data (such as encrypted PIN, container name, reader name, and position information) and sent them back to LogonUI.
6. Data from Logon UI are now presented by Winlogon for LSALogonUser.
7. LSA calls Kerberos Authentication Package (Kerberos SSP) to create a Kerberos Authentication Service Request (KRB_AS_REQ) containing a pre-authenticator [12].
8. The Kerberos SSP sends an authentication request [12] to the Key Distribution Center (KDC) service that runs on a domain controller, to request a Ticket Granting Ticket (TGT).
9. The KDC finds the user's account object in the active directory and uses the user's credentials to verify the user identity.
10. The KDC validates the user's key to ensure that the credential information come from a trusted source.
11. The KDC service retrieves user account information from Active Directory. The KDC constructs a TGT based on the user account information that it retrieves from Active Directory. The TGT includes the user's security identifier (SID), the SIDs for universal and global domain groups to, which the user belongs, and (in a multi-domain environment) the SIDs for any universal groups of, which the user is a member. The TGT's authorization data fields include the list of SIDs.
12. The domain controller returns the TGT to the client as part of the KRB_AS_REP response.
13. The response is as per RFC 4556 [12].
14. The client validates the reply from the KDC (time, path and revocation status).
15. Now that a TGT has been obtained, the client obtains a Service Ticket to the local computer in order to log on to the computer.
16. On success, LSA stores the tickets and returns success to the LSALogonUser. On this success message, user profile, last logon time and position information are obtained.
17. Custom login script for multifactor authentication device is called from AD login policies. The MAD custom script serves as an intelligent decision algorithm, which compares current position with last logon position and last logon time with current time on AD authentication server from Kerberos authentication packet. Using authentication server time prevents changing time cheating. Based on these comparisons user access is allowed or denied.
    a. In case of successful authorization logon process continues normally according to user's policies. Last login time and position in AD is actualized to current values.
    b. If user access is denied Winlogon returns to original state and waits for another user logon attempts.

Preconditions for successful login into AD are customized user's properties in AD extended by login position and time information. These values are validated against position and time of MAD used for user authorization.

Logon UI for the thin client with implemented multifactor authentication is shown in Fig. 8. The thin client doesn't obtain user's credentials from MAD but allows only weakest authorization by three factors. User is challenged for his username and password. These credentials are expanded by the fixed position information of the thin client and AD authorization authority runs modified authorization process, which was described before. Difference of thin and thick client Logon UI implementation is the thick client offers only password input box for entering password. All other necessary information is read from connected MAD (position, username obtained by the biometric validation).

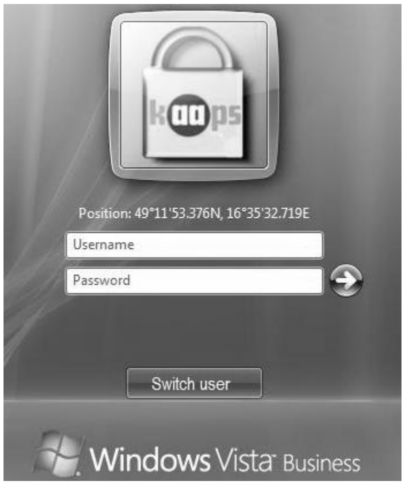
Position: 49°11'53.376N, 16°35'32.719E

Fig. 8. Microsoft Windows Vista logon screens with integrated support of Multifactor Authentication Device (MAD connected-obtained position information, dialog used for user login)

VIII. CONCLUSION AND FUTURE WORK

Common multifactor authentication processes combine in most cases two or three unique authentication factors. Typical scenario is biometric reader connected or inbuilt to personal computer and user is verified by biometrics, and by password knowledge. Similar example is using personal tokens with certificates, when user has to proof knowledge of PIN which secures personal certificate stored in token.

Our newly developed solution combines new multifactor authentication device with currently used technologies as an authentication system based on the Microsoft Credential provider in combination with corporate network with Active Directory services. Main advantages of presented solution are added position information as an extra authentication factor, increased security level due to the position restrictions and rules for allowing or denning access from predefined areas, compatibility with widely used Microsoft technologies and systems and possibility to implement into current corporate networks based on the Active Directory services.

Our future work will be focused on the finishing Multifactor Authentication Device prototype realization and testing in connection with Microsoft Credential provider itself and in combination with Active Directory services under real corporate network.

ACKNOWLEDGMENT

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 ARTEMIS JU in Project No. 100205 Process Oriented Electronic Control Units for Electric Vehicles Developed on a multi-system real-time embedded platform and 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-TI1/057Automatic stocktaking system and FR-TI1/057 Intelligent house-open platform.

REFERENCES

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

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

[3] Schilit, B., et al., *Wireless location privacy protection*, Computer, vol. 36, pp. 135-137, Dec 2003.

[4] Tikamdas, P. S., and El Nahas, A., *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.

[5] Menezes A., et al., *Handbook of Applied Cryptography*, CRC Press, 1997.

[6] Cutler, T. J., *Dutton's Nautical Navigation*, 2003. 664 pages. ISBN 155750248X.

[7] Monahan, K., and Douglass, D., *GPS Instant Navigation: A Practical Guide from Basics to Advanced Techniques*. 2nd edition. Fine Edge Productions, 2000. 333 pages. ISBN 0938665766.

[8] Larson, R., *Geometry*. Houghton Mifflin Harcourt, 2006. 1003 pages. ISBN 0618595406.

[9] Kiaer, M., *Multifactor authentication in Windows - Part 2: Preparing Devices on XP and Windows 2003*. WindowSecurity.com. [Online] 12. 2 2008. [Cited: 17. 6 2009.] http://www.windowsecurity.com/articles/Multifactor-authentication-Windows-Part1.html.

[10] Mysore, S. H. *Windows Vista Smart Card Infrastructure. Microsoft Download Center*. [Online] 16. 8 2007. [Cited: 17. 6 2009.] http://www.microsoft.com/downloads/details.aspx?familyid=AC201438-3317-44D3-9638-07625FE397B9&displaylang=en.

[11] Griffin, D., *Create Custom Login Experiences With Credential Providers For Windows Vista*. MSDN Magazine. [Online] 1 2007. [Cited: 5. 6 2009.] http://msdn.microsoft.com/en-us/magazine/cc163489.aspx.

[12] Zhu, L., and Tung, B., *Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)*. RFC4556. http://www.ietf.org/rfc/rfc4556.txt: Microsoft, June 2006.

[13] Microsoft. *How the Kerberos Version 5 Authentication Protocol Works*. Microsoft TechNet. [Online] May 2008. [Cited: 17. 6 2009.] http://technet.microsoft.com/en-us/library/cc772815.aspx.

[14] Harrison, E. R., *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*. RFC:4513. http://www.rfc-editor.org/rfc/rfc4513.txt: Novell, Inc., 2006.

[15] Melnikov, A., and Zeilenga, K., *Simple Authentication and Security Layer (SASL)*. RFC4422. http://www.ietf.org/rfc/rfc4422.txt: OpenLDAP Foundation, 2006.