2010 Sixth International Conference on Wireless and Mobile Communications

Implementation of an Advanced Authentication Method Within Microsoft Active Directory Network Services

Jaroslav Kadlec, David Jaros, Radek Kuchta
Dept. of Microelectronics, FEEC
Brno University of Technology
Brno, Czech Republic
kadlecja | jarosd | kuchtar @feec.vutbr.cz

Abstract— **This paper describes a new approach for developing and implementing an advanced authentication method within active directory network services. For advance authentication process a new type of user multi-factor authentication based on the classical three-factor authentication extended by the position information and time is described in this paper. The main objectives of our applied research are extended security features for more robust and more secure user's authentication process. Application scenario of advanced multi-factor authentication method within corporate networks based on the Microsoft Active Directory network services is presented. Five different factors for user's authentication provide more secured access control layer for current corporate networks with Microsoft Active Directory with only small implementation costs.**

Keywords- multi-factor authentication; position; credential provide.

I. INTRODUCTION

User identity is the most valuable information in this digital age and person's digital identity has to be trusted all times. Authentication is the process by which end users identify themselves to a network and customized access capabilities are given based on the role they serve in the organization. Policy Manager uses an Active Directory domain server [1, 2], which includes an authentication authority to dynamically assign a policy (or role) to a user or a device, based on the end user's login or MAC (Media Access Control) address. User can be verified by several factors [3]. Conventional authentication systems are based on the one factor authentication typically by the shared secret, e.g. password or PIN (Personal Identification Number). The newest authentication systems add next factor. Smart cards or tokens are quite trustworthy ways for user authentication but can be stolen and abused [4]. On the other hand biometrics can unique identify person with minimal risk of identity replacement. Problem can be with storing biometrics information in digital representation and securing this very sensitive user data to prevent it from possible misuse and also with higher implementation costs [5].

Classic multifactor authentication combines following factors:

- Something you know – password or PIN
- Something you have – token or smart card (two-factor authentication)
- Something you are – biometrics, such as a fingerprint (three-factor authentication)

Five-factor authentication adds another two indicators, which can help to identify users and secure user's sensitive data. The next two factors are:

- Where you are - position information (four-factor authentication)
- When you are – time information (five factor authentication)

Time can limit locking of the user's account. If the user has fixed working time than accessibility of user's account in another time except regular working time is unwanted. The same situation is with position. System administrator can restrict login area only to several locations for example user's office or company buildings. Combination of these two additional factors provides one more advantage. If a user logoffs in his office and next request to login is from another city or country five minutes later it is probably attempt to attack user's account. Position also can serve for authorization to restrict accessibility of confidential data only to fix location, e.g. user's office. Knowledge of user's working times and locations, gives us another possibilities how to secure his account and prevent possible attacks to his private credentials [6].

In the paper, a basic application scenario is described in second section. Next section describes implementation to the Microsoft Windows Vista Credential Security Service Provider and, at the end of the paper, future work and conclusions are described.

II. APPLICATION SCENARIO

Our application of five factor authentication is divided into the three basic levels. The first level is the most robust implementation on a thick client. The thick client has connected MAD (Multifactor Authentication Device), which provides biometrical user identification and information about current position. A user can logon through the thick client to the network by all five factors and connection to AD (Active Directory) controller is the most trusted. AD controller verifies user's credentials and according to user's

978-0-7695-4182-2/10 $26.00 © 2010 IEEE
DOI 10.1109/ICWMC.2010.48

current location and time on the AD controller sets user's policies and access rights.

The second level is not so secure level without MAD connected to a thin client. The thin client has in his AD profile fixed location, which is used for all logon requirements from it. A user is verified only by login and password. In this case only three factors are used (shared knowledge, location and time). Therefore implementation of the thin client can be done only to trustworthy computers.

Third level is implementation in area with wireless localization. Complete application scenario is shown in Figure 1.

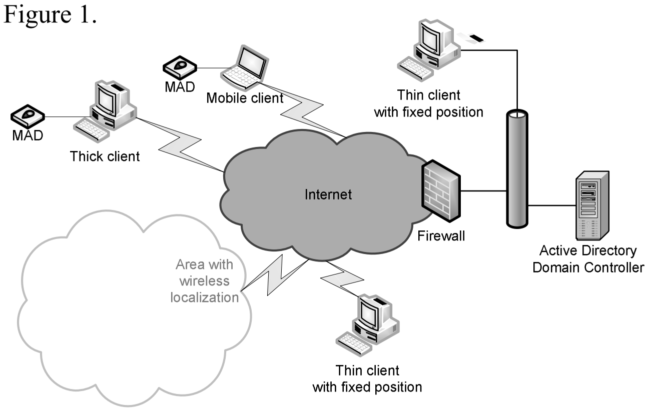

Figure 1. Application scenario of multifactor implementation

III. 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 [7].

Credential providers [7] are in-process COM (Component Object Model) objects that are used to collect credentials in Windows Vista and run in local system context. In summary, the logon UI (User Interface) 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 [10, 11, 12, 13].

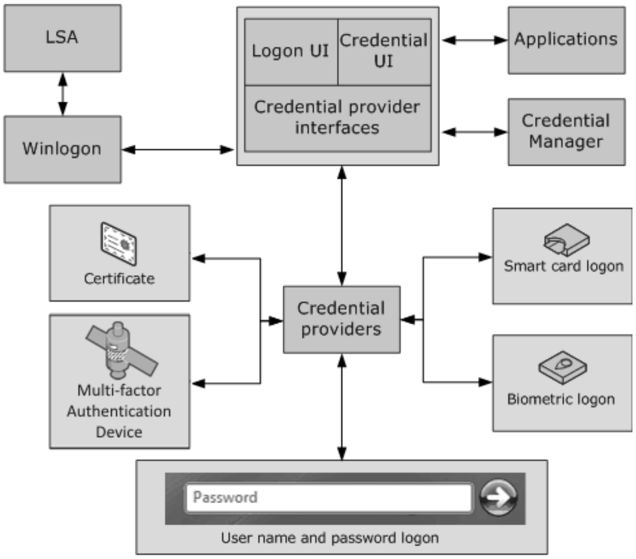

Figure 2. Windows Vista hybrid credential provider architecture with integrated MAD CredSPP [8]

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.

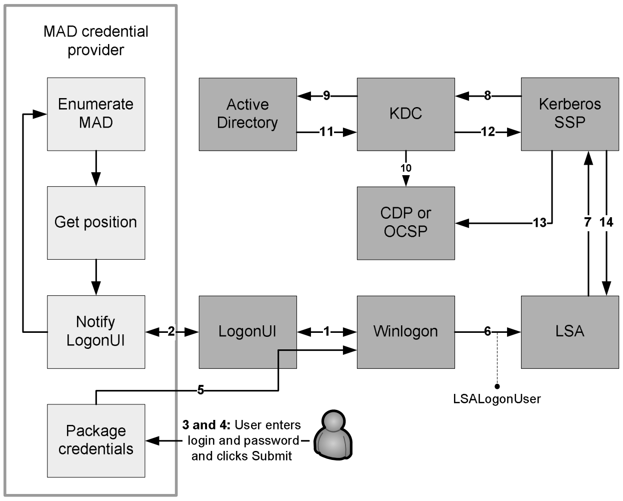

Figure 3. Modified logon flow [8] for MAD authentication process

The hybrid credential provider architecture is shown in Figure 2. The hybrid credential provider API (Application

Programming Interface) does not design UI 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.

IV. 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 [9]. Flow sequence of logon process within Multifactor Authentication Device (see Figure 3):

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.
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 [10].
8. The Kerberos SSP sends an authentication request [10] 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.
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 Figure 4. The thin client does not 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).

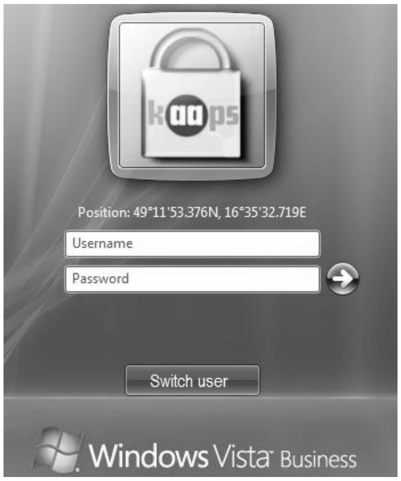
Position: 49°11'53.376N, 16°35'32.719E

Figure 4. Microsoft Windows Vista logon screens with integrated support of Multifactor Authentication Device (MAD connected-obtained position information, dialog used for user login)

V. FUTURE WORK AND CONCLUSIONS

In the paper, a new idea of multi-factor authentication process extended by position information and time were described. Our main research effort was focused on the application scenarios of user authentication process extended by two new factors and implementation this new approach to the currently used corporate networks. For implementation of this new multi-factor authentication method we chose Microsoft Active Directory as one of the most used corporate network technologies.

Currently we are working on design of new authentication devices that will provide additional user's authentication data. We are also preparing new authentication modules for Microsoft servers that allow to process and set authentication policies for new designed multifactor authentication techniques.

The paper was mainly focused to the description of basic use-cases of five-factor authentication process and description of possible way of implementation into the newest network authentication process' structure. Developed solution of authentication with the help of position information described in the paper is mainly focused to the field of corporate networks but it could be also used in many different applications.

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 the Czech Ministry of Industry and Trade in the project FR-TI1/057 *Automatic stocktaking system*, partly supported in the project GA 102/09/1897 *Car Transport Safety – BAD* and in the 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.

REFERENCES

[1] Shin, J., W., Park, S., T., and Hwang, C., S.: Domain-based Key Management Scheme for Active Network, Proceedings of World Academy of Science, Engineering and Technology, no. 14, pp. 33-36, Aug. 2006, ISSN: 1307-6884.

[2] Koshutanski, H., Lazouski, A., Martinelli, F., and Mori, P.: Enhancing grid security by fine-grained behavioral control and negotiation-based authorization, International Journal of Information Security, vol. 4, no. 8, pp. 291-314, Aug. 2009, ISSN: 1615-5262.

[3] Wang, L., W., He, L., Y., Liao, X., K., and Wang, H., M.: Research on control flags-based weighted authentication trustworthiness model, 11th Pacific Rim International Symposium on Dependable Computing, Proceedings, no. 1, pp. 369-373, Dec. 2005, ISBN: 0-7695-2492-3.

[4] Falk, R., Goudalo, W., Chen, E., Y., Savola, R., and Popescu, M.: Multi-level Authentication Scheme Utilizing Smart Cards and Biometrics, 3rd International Conference on Emerging Security Information, Systems and Technologies, no. 1, pp. 93-98, Jun. 2009, ISBN: 978-1-4244-4308-6.

[5] Sutcu, Y., Li, Q., and Memon, N.: Protecting biometric templates with sketch: Theory and practice, IEEE Transactions on Information Forensic and Security, vol. 3, no. 2, pp. 503-512, Sep. 2007, ISSN: 1556-6013.

[6] Zhang, Y., C., Liu, W., Lou, W., J., and Fang, Y.-G.: Location-based compromise-tolerant security mechanisms for wireless sensor networks, IEEE Journal on selected areas in communications, vol. 2, no. 24, pp. 247-260, Feb. 2006, ISSN: 0733-8716.

[7] 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.

[8] 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.

[9] Griffin, D.: Create Custom Login Experiences With Credential Providers For Windows Vista. *MSDN Magazine.* [Online] 7. 1. 2007. [Cited: 5. 6 2009.] http://msdn.microsoft.com/en-us/magazine/cc163489.aspx.

[10] 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.

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

[12] 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.

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