ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2015
Seria: ORGANIZACJA I ZARZĄDZANIE z. 86 Nr kol. 1946

Adrian KAPCZYŃSKI
Politechnika Śląska
Wydział Matematyki Stosowanej
adrian@polsl.pl

CHALLENGING THE PROBLEM OF AUTHENTICATION OF USERS PARTICIPATING IN BLENDED STRATEGY MEETINGS

Summary. In the paper the problem of user authentication participating in strategy meetings conducted in blended type (VM and F2F) is addresses. In the first part of the paper the strategy meetings are briefly characterized, with reference to real organization from IT industry. The second part of the paper is devoted to authentication methods and the basics related to evaluation of its performance. The third part is about the novel approach related to user authentication participating in blended-type meeting.

Keywords: authentication, blended strategy meetings.

PODJĘCIE PROBLEMU UWIERZYTELNIANIA UŻYTKOWNIKÓW UCZESTNICZĄCYCH W SPOTKANIACH STRATEGICZNYCH REALIZOWANYCH W FORMULE MIESZANEJ

Streszczenie. W artykule podjęto zagadnienie uwierzytelniania użytkowników biorących udział w spotkaniach strategicznych, realizowanych w formule mieszanej. W pierwszej części artykułu krótko scharakteryzowano spotkania strategiczne, realizowane w formule mieszanej, odnosząc się do rzeczywistej organizacji z branży IT. Druga część artykułu poświęcona jest metodom uwierzytelniania i podstawami oceny ich wydajności. Trzecia część dotyczy nowego podejścia związanego z uwierzytelnianiem użytkownika, uczestniczącego w spotkaniach w formule mieszanej.

Słowa kluczowe: uwierzytelnianie, spotkania strategiczne w formule mieszanej.

1. Introduction

The motivation for the research in the field of user authentication in blended type strategy meetings have formulated from both academic and professional reasons. It is definitely an interdisciplinary area of interest, with deep connection in human interaction, communication, management and computer science. The literature review [1, 8, 12] shows general awareness of the threats, vulnerabilities and the countermeasures concerning the assets and performed processes during the meetings of virtual teams. The observation of out-of-laboratory environment brings into consideration the complementary type of the meetings to physical meetings and virtual meetings: the blended-type meetings, which combine the previously mentioned types of the meetings (there are participants who are physically present and the participants who are present virtually (remotely)).

The goal of the paper is to formulate the challenge of user authentication participating in blended-type strategy meeting and introduce the concept that addresses that challenge.

The article has been divided into three parts with introduction at the beginning and summary at the end. The first part is about strategy meetings, the second part is about authentication methods and the third part is about the novel approach related to user authentication.

2. Strategy meetings – personal, virtual and blended

From theoretical [8] and practical points of view, there are three major types of meetings divided due to the criterion of presence of the participant:

- physical meeting (all participants are attending the meeting in person, further called as F2F (Face-to-Face)),
- virtual meeting (all participants are not physically present in the meeting location, abbreviated VM),
- blended meeting (combination of physical type and virtual type, abbreviated BM).

In this paper the further consideration is focused on meetings devoted to strategic-level aspects related to given, existing (real) organization from IT industry.

In that organization, the meetings are organized in all of types mentioned above: the operational and tactic meetings are realized as physical or virtual meetings and the strategy meetings are organized in blended formulae. The reason for this is related with international nature of the body that is supervising the management board and of course due to the economic aspect of travels to headquarter of the company (which is located in Poland), i.e. the

place, where strategy meetings are held. The meetings are held in conference room equipped with unified collaboration system [3] that enables multi-way communication with high-definition telepresence technology.

During the meetings there is a redundant way of communication utilizing only text and voice communication channels. The conference room is equipped with unified collaboration system that has been presented on fig. 1 (the meeting took place on 30.09.2015 in Katowice, Poland).

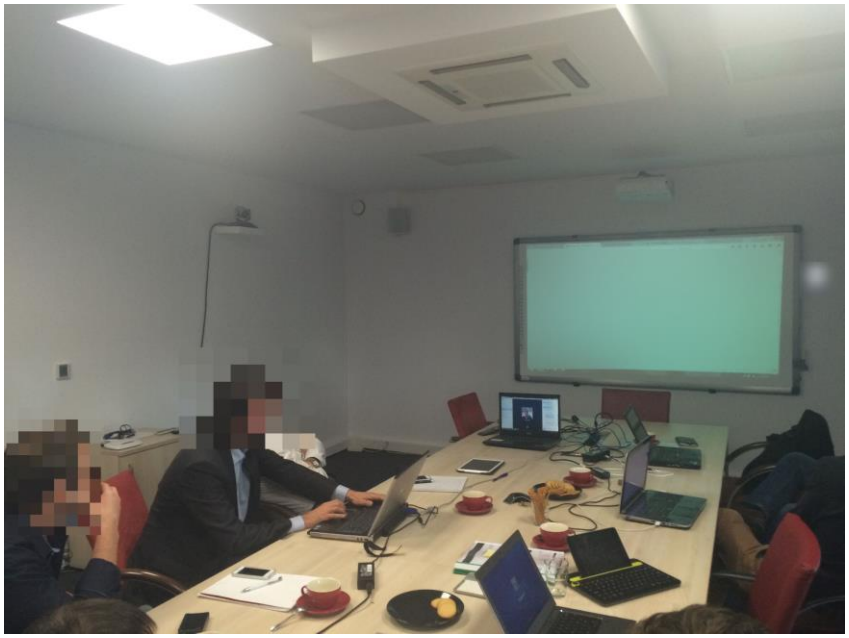

Fig. 1. Strategy meeting held in conference room equipped with unified collaboration solution
Rys. 1. Spotkanie strategiczne w sali konferencyjnej, wyposażonej w rozwiązanie z zakresu zunifikowanej komunikacji
Source: author's own.

Participants who are physically present are authenticated to access the meeting collaboration area by username and password and the same way is applied to those participants who are participating remotely (even those who are not able or not willing to use videoconference system). Such approach has a great potential of improvement, which will be addressed shortly after description of authentication methods and basics of their performance evaluation.

3. Authentication methods

In the scientific and technical literature there are highlighted four main types of authentication methods [4, 6, 10]:

1. The authentication methods based on the knowledge of users (Something you know).
2. The authentication methods based on the physical identifiers (Something you have).
3. The authentication methods based on biological characteristics (Something you are).
4. The authentication methods based on action (Something you do).

Among the methods based on the user's knowledge, one of the most popular is the method based on knowledge (confidential password). A password could be understood as a string selected by the user from the password alphabet. The security level of the password is proportional to the number of characters in the alphabet password, since it is the power of the alphabet (N) and the password length (L) and depends on the complexity of the attack. In order to reduce the negative effects of revealed password the period of its validity is shortened. It seems that the most effective way to minimize this threat consequences, is to use one-time password system. Time passwords may be generated by the user or by the generator in a manual or automatic way. It is recommended that during the process of transport, processing and storage the passwords must be encrypted using one of cryptographic algorithms (e.g. RSA). Passwords are often stored after transformation by one-way hash function. The level of security could be increased through the creation of log entries history or the regular examination of passwords strengths. The main disadvantage is the susceptibility (despite using one-way functions) to dictionary attacks.

An alternative to methods based on knowledge are the methods based on physical identifiers. The role IDs can perform the simplest example in the construction (and cheapest) memory cards or smart cards. Next to the memory cards used cards are also equipped with a microprocessor, as well as super-intelligent cards, additionally equipped with a miniature screen and alphanumeric keypad. The electronic card is characterized by high resistance to the influence of external fields, including electromagnetic and electrostatic. During the identification process the information contained on the card can be read by contact or contactless reader. In the latter case, the transmission is performed using inductive coupling, infrared or radio. The main disadvantage of systems based on the material IDs, it is possible that they are lost, stolen or counterfeit.

The authentication methods based on biological characteristics of users and methods based on user actions, referred to collectively as biometric methods, use the uniqueness of selected anatomical and behavioral traits. The authentication process is most commonly based on [2] fingerprints of the fingers, hand shape, voice or the way of typing (keystroke dynamics).

Complemented to presented basic types of authentication methods that use basic factors (something that is familiar, something that one’s have, something what one is and what one is doing) are the authentication methods using hidden factors: authentication based on geodetic (physical) location and authenticate based on a logical location, which can be used in supporting authentication processes (e.g. by the Internet).

In this paper we will focus on biometric authentication as an alternative to knowledge-based authentication which is currently used during the strategy meetings of given organization.

The biometric authentication systems operates in two phases: enrollment and verification [1].

During the first phase (noted as Phase A) raw biometric data is preprocessed, later transformed into set of features and finally stored with user identifier in biometric template database (see fig. 2).

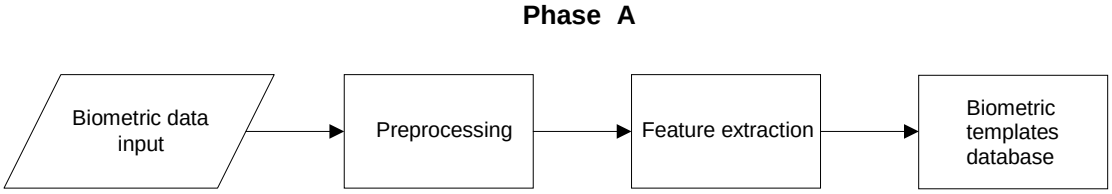

Fig. 2. Biometric authentication – phase A (enrollment)
Rys. 2. Uwierzytelnianie biometryczne – faza A (rejestracja)
Source: author's own based on [2].

The verification phase (noted as Phase B) is aimed at answering the question whether the authentication data provided by the user is positively or negatively verified against data stored in biometric template database created during the enrollment phase. In Phase B, the authentication data consists of raw biometric data and user identifier which is used during the comparison – the corresponding to user identifier reference template is selected from biometric template database and compared with the result of extracted feature set created from current raw biometric data, i.e. the biometric data provided by the user during the verification phase (see fig. 3). Without the use of identifier it will not be the authentication problem, but the identification problem (which is out of the scope of this paper).

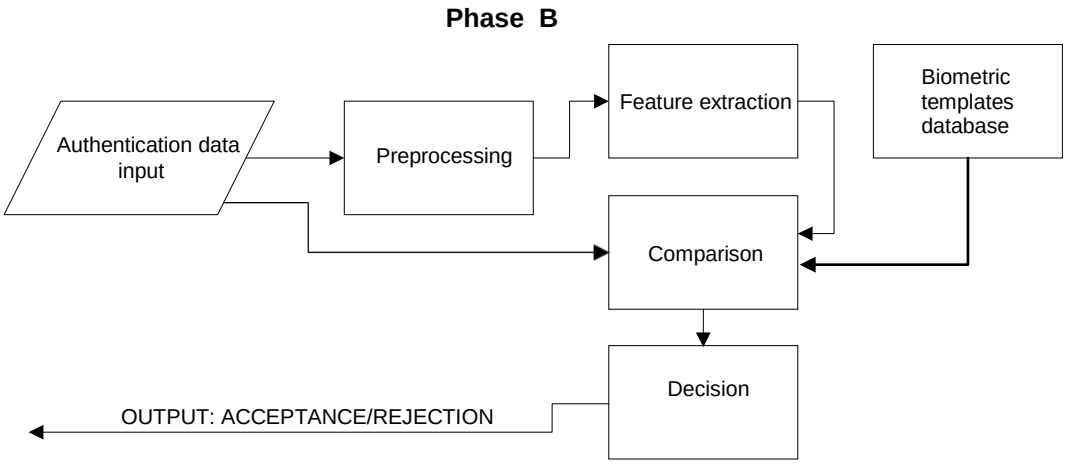

Fig. 3. Biometric authentication – phase B (verification)
Rys. 3. Uwierzytelnianie biometryczne – faza B (weryfikacja)
Source: author's own based on [2].

Biometric authentication system produces an output which could be correct or not correct according to expected results i.e. the authentication attempt performed by legitimate user (so called true attempt) shall by accepted and the authentication attempt performed by the impostor (so called false attempt) shall be rejected [11].

We have therefore two classes: the positive class (noted as PC) and the negative class (noted as NC). Two distributions: impostor (NC) and genuine (PC) are presented on the graph (fig. 4), where OY axis is probability P and OX axis is matching score M and T is the threshold of the biometric system [5, 7].

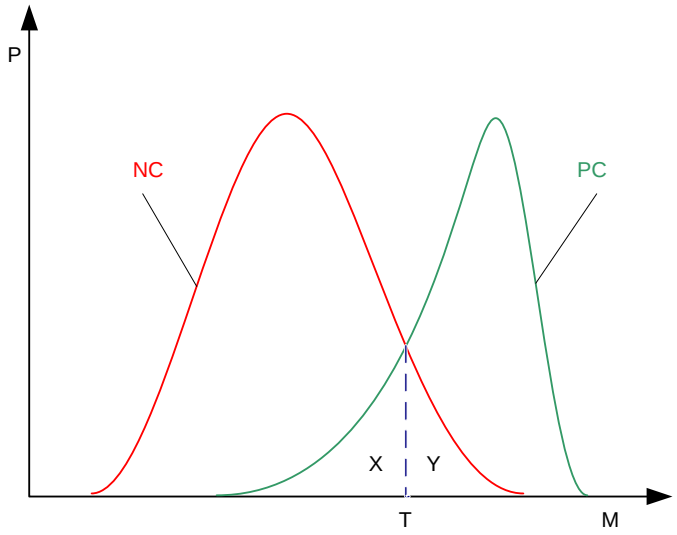

Fig. 4. Biometric system FAR/FRR diagram
Rys. 4. Diagram błędnych akceptacji/błędnych odrzuceń systemu biometrycznego
Source: author's own based on [9].

The area X presents cases of incorrect rejection, while area Y shows instances of incorrect acceptance. When the threshold value is increased the probability of an erroneous acceptance decreases, while the probability of erroneous rejection increases. The conclusion is that it is not possible to minimize the probability of false acceptance at the same time minimizing the probability of false rejection.

Due to the possibility of the above results there are two main indicators characterizing the performance of the biometric system [9]: false rejection rate (FRR) and false acceptance rate (FAR).

False rejection rate, also known as the error rate of the first type, is defined as the probability that a legitimate user is classified as an impostor and is expressed by the formula (1):

$$FRR = \frac{FR}{TTA} \cdot 100\% \tag{1}$$

where:

FRR – false rejection rate

FR – number of attempts falsely rejected

TTA – number of total true attempts (performed by legitimate users)

False acceptance rate (also known as the error rate of the second type) is defined as the probability that an impostor is classified as the legitimate user and is expressed by the formula (2):

$$FAR = \frac{FA}{TFA} \cdot 100\% \tag{2}$$

where:

FAR – false acceptance rate

FA – number of attempts falsely accepted

TFA – total number of false attempts

As noted, the desire to minimize one indicator, typically leads to an increase of the second indicator. It is important to set the appropriate biometric system threshold (T).

Performance evaluation can also be performed based on a determination of the degree of separation between the distributions of positive and negative population (d') based on appropriate means and standard deviations, using a formula (3).

$$d' = \frac{\left\| M_{NC} - M_{PC} \right\|}{\sqrt{(SD^2{}_{NC} + SD^2{}_{PC}) \cdot 0{,}5}}, \tag{3}$$

where:

M_{NC} – the average of the distribution of the negative population

M_{PC} – the average of the distribution of the positive population

SD_{NC} – standard deviation of the distribution of the negative population

SP_{PC} – standard deviation of distribution of positive population

In next part of the article the author's own approach of using biometric authentication methods during strategy meetings is presented.

4. Authentication methods in blended strategy meetings

The proposed approach of authentication of users participating in blended meetings relies on:

- a requirement that all users regardless whether they are physically present or using the videoconference system or any other mean of computer-assisted communication, will be required to start the interaction with captive portal, which consists of opening session, main session and closing session; during the opening session and closing session the attributes related to user's environment are verified against authentication profile, created during the supervised enrollment (e.g. including time, location, device type, etc.);

- using enhanced user authentication, that means that all of the participants will be using keystroke dynamics as an additional authentication mechanism to currently used authentication mechanism which is relying on user name and password;
- running the authentication phases in continuous mode from the beginning of the meeting till the end of the meeting.

5. Summary

This paper presents the opening insights of addressing the user authentication which are participating in blended-type strategy meetings. It the first part of the article the research context has been presented, which was inspired by real-life strategy meetings of supervisory board of existing organization with headquarters located in Poland. In second part, the authentication methods were described and in the third part, the novel approach to user authentication participating in blended-type meetings.

As the concept phase has been completed, the research work could be performed in the area of empirical verification of proposed approach. That will be the next step which scientific implications will be elaborated in the separate paper.

Bibliography

1. Anderson A.H., Mcewan R., Bal J., Carletta J.: Virtual team meetings: An analysis of communication and context. Computers in Human Behavior, 23, 2007.
2. Ashbourn J.: Biometrics. Advanced Identity Verification. Springer-Verlag, 2000.
3. Chen K., Lien S.: Machine-to-machine communications: Technologies and challenges. Ad Hoc Networks, Vol. 18, 2014.
4. Dissanayaka A., Annakkage U.D., Jayasekara B., Bagen B.: Risk-based dynamic security assessment. Power Systems, IEEE Transactions on, Vol. 26, No. 3, 2011.
5. Jain A.K., Bolle R., Pankanti S.: Biometrics. Personal identification in networked society. Kluwer Academic Publishers, 2000.
6. Lampson B.W., Abadi M., Burrows M., Wobber E.: Authentication in distributed systems: theory and practice. ACM Transactions on Computer Systems, Vol. 10, No. 4, 1992.
7. Liu S., Silverman M.A.: Practical guide to biometric security technology. IEEE Computer Society Journal, 2002.
8. Lurey J.S., Raisinghani M.S.: An empirical study of best practices in virtual teams Information and Management, 38, 2001.

9. Nanavanti S., Thieme M., Nanavati R.: Biometrics - identity verification. Wiley & Sons, Inc., 2002.
10. Pipkin D.: Information security: protecting the global enterprise. Prentice Hall, Inc. 2000.
11. Tistarelli M., Bigun J., Jain A.: Biometric Authentication. Springer-Verlag, 2002.
12. Wong S.S., Burton, R.M.: Virtual Teams: What are their characteristics and impact on team performance? Computational and Mathematical Organization Theory, 6, 2000.

Omówienie

W artykule autor przybliża zagadnienia związane z uwierzytelnianiem użytkownika w czasie mieszanych spotkań strategicznych. W tych spotkaniach uczestniczą dwa rodzaje uczestników: uczestnicy, którzy są fizycznie obecni oraz ci, którzy są obecni wirtualnie. Pierwszy punkt artykułu obejmuje krótkie wprowadzenie do głównego przedmiotu poruszanego w artykule, który obejmuje: genezę, cel opracowania oraz jego zakres. W kolejnej części artykułu krótko scharakteryzowano formułę mieszanych spotkań strategicznych, ze szczególnym naciskiem na potrzeby związane z uwierzytelnianiem użytkowników biorących udział w posiedzeniu. Trzecia część artykułu poświęcona jest uwierzytelnianiu użytkownika z uwzględnieniem metod biometrycznych uwierzytelniania, w tym oceny skuteczności ich funkcjonowania. Wreszcie autor przedstawia nowe podejście uwierzytelniania użytkowników uczestniczących w spotkaniach strategii, realizowanych w formule mieszanej. Ostatnia część artykułu składa się z podsumowania oraz opisu kolejnych prac badawczych.