Adrian KAPCZYŃSKI
Politechnika Śląska, Katedra Informatyki i Ekonometrii

MODELING BIOMETRIC AUTHENTICATION SYSTEMS

Summary. In the paper basics of BANTAM were presented as well as an example of practical application of it in modeling of biometric authentication system constructed according to provided assumptions.

Keywords: biometric, authentication, BANTAM.

MODELOWANIE BIOMETRYCZNYCH SYSTEMÓW UWIERZYTELNIANIA

Streszczenie. W artykule zostały przedstawione podstawy języka BANTAM, jak również przykład praktycznego jego zastosowania do modelowania biometrycznego systemu uwierzytelniania skonstruowanego według przyjętych założeń.

Słowa kluczowe: biometryka, uwierzytelnianie, BANTAM.

1. Introduction

Authentication issues are nowadays of utmost importance. Every IT security solution shall be built after careful consideration of quality of chosen authentication protocols involved during communication and chosen authentication methods of users who may have access to sensitive data.

Authentication methods applied in standalone or network environments should guarantee accurate automatic identification or authentication of users. That means neither false acceptance of impostors nor false rejection of genuine ones.

It turns out that shared secrets such as PINs or passwords or even a key devices like smart cards just are not enough in high-security applications. What is needed is something that could verify that there is physically the person he or she claims to be – "biometrics". This term refers

strictly speaking to a science involving the statistical analysis of biological characteristics. In this article "biometrics" is used in a context of analyzing human characteristics for security purposes, and can be defined as a unique, measurable characteristics or trait of a human being for automatically recognizing or verifying identity [1].

It is believed that biometric methods are to be one of the strongest of all authentication methods ever applied. However, one should be aware of the fact that many technical, economical and social requirements shall be met in order to achieve the status declared above.

From technical point of view it is very important to analyze the architecture of biometric authentication systems and possible threats on different levels of abstraction. Especially for security officers or other staff responsible for designing, implementation and support of secure authentication systems it is truly vital to have tools that will enhance their capabilities in realizing their tasks.

One of the means that can help is BANTAM – a biometric specific methodology to help the end user or systems consultant to capture the requirement in a manner that can be easily translated into systems design.

The basics of that language as well as an working example will be provided after short introduction into biometrics domain.

2. Biometric systems primer

One of the most dangerous security threats is the impersonation, in which somebody claims to be somebody else. The security services that counter this threat are identification and authentication. Identification is the service where an identity is assigned to a specific individual, and authentication the service designed to verify a user's identity. The verifier can be identified and authenticated by what he knows (e.g. password), by what he owns (e.g. smart card) or by his human characteristics (biometrics).

Biometric systems verify a person's identity by analyzing his physical features or behaviors. The first group of methods measures the physiological characteristics of a person (fingerprint verification, iris analysis, facial analysis, hand geometry-vein patterns, ear recognition, odor detection, DNA pattern analysis and sweat pores analysis. The latter group, i.e. behavioral based techniques, measures the behavior of a person (handwritten signature verification, keystroke analysis and speech analysis).

There are two basic concerns in these technologies: the error tolerance and the storage of the templates. The setting of the error tolerance of these systems is critical to their

performance [1]. Both errors (False Rejection and False Acceptance) should be low and they should both be quoted by the manufacturers.

The recorded biometric measurement of a user (template) can be stored in various places depending on the application and the security requirements of this application. The templates can be stored in the biometric device, in a central data base or in plastic cards. Trusted third party services can provide security in transmitting and managing the templates when stored in a central database.

Reliability and acceptance of a security system depends on how the system is protected against threats and its effectiveness to identify system's abuses.

Keeping in hand with the latter attribute it shall be emphasized that novel approach basing on multiple biometric authentication system was introduced in [3] by the Author. In order to properly present and analyze anatomy of multiple biometrics authentication system, a new easy-in-use methodology was needed. The only one that has appeared and has met the requirements is called BANTAM [2].

In next chapter there will be a brief description of BANTAM provided as well as complete set of BANTAM symbols used in example shown in proceeding paragraph.

3. BANTAM language basics

BANTAM stands for Biometric and Token Technology Application Modeling Language. It's a methodology which facilitates the definition of application requirements, operational processes, logical systems design, functional systems design and also object relationships [2]. In order to translate easily between desired and deliverable system, like many contemporary software design systems, BANTAM is using an object oriented methodology.

BANTAM has been designed around a core set of objects which may be used within a graphical context to represent the application's functionality requirements. Objects within BANTAM may have attributes, which can be described or elaborated within the accompanying text of any BANTAM model.

Resulting diagrams may be used to illustrate process flow, systems operation and other aspects. Whilst BANTAM may be extensible, it is essentially conceived as a simple, intuitive language to be easily used with minimal familiarization.

The standard BANTAM methodology is freely available under an open distribution model, which allows distributing BANTAM both to internal departments and other organizations in order for them to liaise on projects using BANTAM.

The standard distribution includes the following components: introductory guide, the BANTAM symbol selector software, the symbol library in bitmap format and a full set of document templates in Microsoft Word format. In addition there is available an optional software component which provides tools for project logging and document management.

In figure 1 main symbols used in building BANTAM diagrams were gathered.

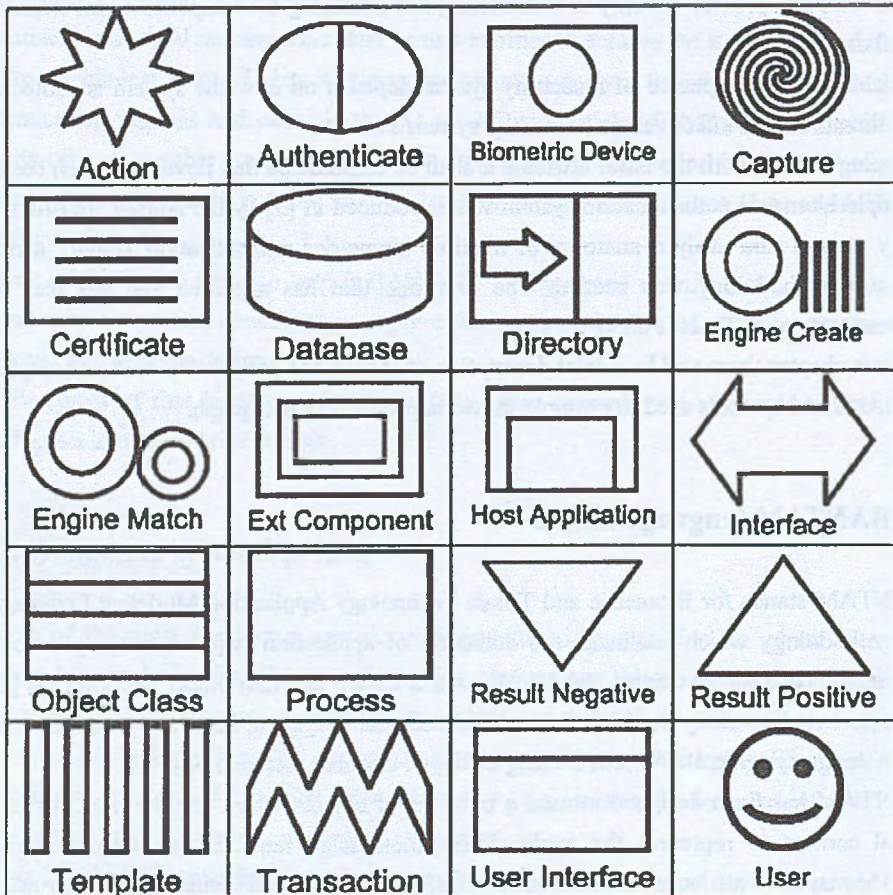|			
Action	Authenticate	Biometric Device	Capture
Certificate	Database	Directory	Engine Create
Engine Match	Ext Component	Host Application	Interface
Object Class	Process	Result Negative	Result Positive
Template	Transaction	User Interface	User

Fig. 1.   BANTAM core elements
Rys. 1.   Podstawowe elementy BANTAM

Presented elements connected in chosen way will let designer obtain the following components:

- applications logic map,
- system architecture map,
- logical scenario map,

    – functional scenario map,

    – object association map,

    – miscellaneous definition map.

Enumerated components can be built using standard BANTAM distribution which consists of templates, utilities and BANTAM guide. The last one contains detailed description of all presented core elements as well as examples of documentation that shall be provided according to methodology.

4. Example of BANTAM language application

As a fulfillment to theoretical aspects concerning biometrics and BANTAM an illustrated example to selected scenario will be supplied below.
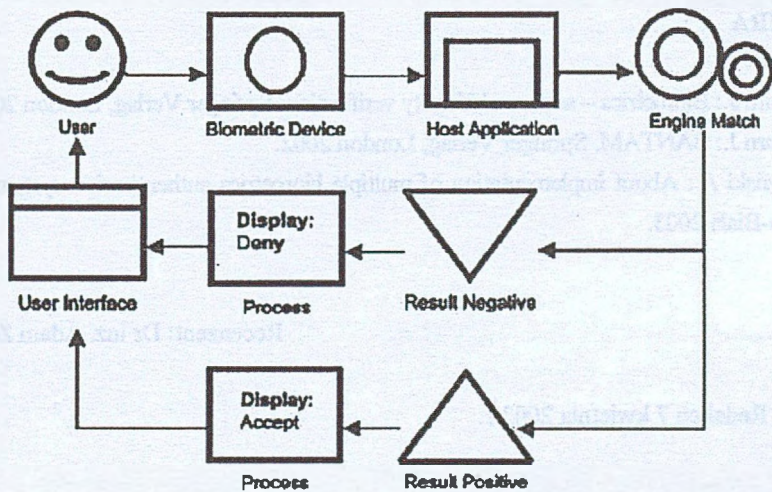

Fig. 2.   Example o Application Logic Map
Rys. 2.   Przykład mapy logiki aplikacji

In figure 2 very simple scenarios is depicted: the user interacts with biometric device which communicates with host application. A matching process is undertaken which produces positive or negative result, each of which sends a message to the user interface.

5. Conclusions

For any biometric or related application, being able to concisely articulate the requirements and attendant processes is important, if a well conceived system is to be designed, implemented and supported.

BANTAM helps the end user or systems consultants to capture the requirement in a manner that is easily translated to systems design with the provision of a high level, simple to use language.

BANTAM has been developed primarily for biometric and token technology applications, but in fact may be used across a much broader range of applications as desired, in order to bring clarity and consistency to the definition, design and implementation of operational projects.

LITERATURA

1.   Ashbourn J.: Biometrics – advanced identity verification. Springer Verlag, London 2000.
2.   Ashbourn J.: BANTAM. Springer Verlag, London 2002.
3.   Kapczyński A.: About implementation of multiple biometrics authentication system. PKSJ, Bielsko-Biała 2003.

Recenzent: Dr inż. Adam Ziębiński

Omówienie

W artykule zostały przedstawione podstawy języka modelowania systemów uwierzytelniania, opartych na materialnych identyfikatorach, oraz cechy anatomiczne i behawioralne.

Zaprezentowano podstawy biometrycznych systemów uwierzytelniania oraz dokonano klasyfikacji metod w nich wykorzystywanych. Wyróżniono metody badające cechy anatomiczne oraz metody badające cechy behawioralne. Dla każdej z grup przytoczone zostały przykłady.

Zarysowano również obszary problemowe związane z bezpieczeństwem przechowywanych wzorców biometrycznych oraz skutecznością kompleksowo traktowanego systemu uwierzytelniania parametryzowanego biometrycznie.

W dalszej części pracy omówiono podstawy języka modelowania BANTAM wraz z wyszczególnieniem elementów podstawowych niezbędnych przy tworzeniu diagramów dla map powiązań logicznych oraz map powiązań funkcjonalnych.

Praktyczny przykład stanowi uzupełnienie teoretycznych kwestii przedstawionych w poprzednich punktach artykułu.

Adres

Adrian KAPCZYŃSKI: Politechnika Śląska, Katedra Informatyki i Ekonometrii, ul. Roosevelta 26-28, 43-800 Zabrze, Polska, adriank@ps.edu.pl.