STUDIA INFORMATICA 2002
Volume 23 Number 2B (49)

Adrian KAPCZYŃSKI
Politechnika Śląska, Katedra Informatyki i Ekonometrii

IMPLEMENTACJA SYSTEMU BIOMETRYCZNEGO W ŚRODOWISKU MS WINDOWS 2000

Streszczenie. W pracy zaprezentowano charakterystyki najczęściej stosowanych metod uwierzytelniania oraz przedstawiono uzyskane dotychczas wyniki badań ukierunkowanych na sformułowanie modelowego rozwiązania systemu uwierzytelniania parametryzowanego biometrycznie. Teoretyczne rozważania zostały uzupełnione wnioskami wynikającymi z praktycznych testów konkretnych sprzętowo-programowych rozwiązań biometrycznych, przeprowadzonych w środowisku systemu operacyjnego Microsoft Windows 2000.

BIOMETRIC AUTHENTICATION SYSTEM IMPLEMENTATION IN MICROSOFT WINDOWS 2000 ENVIRONMENT

Summary. In paper characteristics of most popularly applied authentication methods were described as well as for the time being research notes directed to construct model of biometric authentication system. Theoretical aspects along with conclusion withdrawn from practical tests of specified hardware-software biometric solutions running in Microsoft Windows 2000 environment were provided.

1. Wprowadzenie

Współczesne systemy komputerowe wymagają stosowania skutecznych mechanizmów weryfikacji tożsamości ich użytkowników na podstawie dostarczonych informacji. Uwierzytelnianie stanowi podstawę nadania odpowiednich uprawnień do wykonania określonych działań w systemie, tj. autoryzacji. Rosnące wymagania w zakresie bezpieczeństwa, czasu realizacji oraz innych potrzeb generowanych ze strony użytkowników, przyczyniają się do konieczności znalezienia nowych rozwiązań spełniających te wymogi. Proces uwierzytelniania realizowany jest zwyczajowo na podstawie przedstawionego

identyfikatora oraz hasła, którego znajomość jest weryfikowana. Hasło stanowi element decydujący o sile zabezpieczenia dostępu do określonych zasobów, w szczególności poprzez swoją długość czy stopień skomplikowania. Naturalną tendencją jest stosowanie mechanizmów wymuszających odpowiedni stopień skomplikowania hasła, co wpływa na pogorszenie parametrów procesu uwierzytelniania związanych z czasem jego trwania, stopniem wygody czy też poziomem akceptacji ze strony użytkowników.

W przypadku tej metody weryfikowany jest nie sam użytkownik, lecz posiadana przez niego wiedza. Możliwa jest sytuacja podsłuchania bądź ujawnienia hasła osobie niepowołanej oraz wykorzystania go celem uzyskania dostępu, co w rezultacie doprowadzi do przeprowadzenia procesu błędnej akceptacji (uwierzytelnienia osoby niepowołanej jako prawowitego użytkownika).

Próbą zniwelowania słabości metody opartej na wiedzy jest metoda uwzględniająca materialne identyfikatory, weryfikująca posiadanie określonego obiektu (np. karta procesorowa) oraz znajomość hasła dostępowego. Podobnie jak w przypadku metod opartych na wiedzy, występuje nadal wysokie prawdopodobieństwo realizacji procesu błędnej akceptacji.

Uzupełnieniem rodziny metod opartych na wiedzy i posiadaniu są metody weryfikujące tożsamość na podstawie cech anatomicznych oraz behawiorialnych człowieka. Cechy te, dzięki swym właściwościom, takim jak uniwersalność, unikatowość, trwałość, pozwalają na realizację procesu uwierzytelniania uniezależniając od problemów związanych z koniecznością pamiętania hasła czy też ryzyka utraty materialnego identyfikatora.

Rozwijany w pracy nurt tematyczny obejmuje swoim zakresem podstawowe zagadnienia związane z realizacją procesu uwierzytelniania, przy czym szczególny nacisk położono na badanie grupy silnych metod uwierzytelniania, wykorzystujących charakterystyczne cechy anatomiczne oraz behawioralne użytkowników. Głównym celem pracy jest prezentacja charakterystyki stosowanych metod uwierzytelniania oraz przedstawienie uzyskanych dotychczas wyników, które stanowiły przesłankę prowadzenia dalszych działań, ukierunkowanych na sformułowanie modelowego rozwiązania systemu uwierzytelniania parametryzowanego biometrycznie. Teoretyczne rozważania zostały uzupełnione wnioskami wynikającymi z praktycznych testów konkretnego sprzętowo-programowego rozwiązania systemu biometrycznego, przeprowadzonych w środowisku systemu operacyjnego Microsoft Windows 2000.

2. Uwierzytelnianie użytkowników systemów komputerowych

Procesy uwierzytelniania użytkowników systemów komputerowych związane są z wykorzystaniem metod, które dzielą się na metody oparte na wiedzy użytkowników, np. hasła (ang. *Something you know*), metody oparte na materialnych identyfikatorach, np. kartach procesorowych (ang. *Something you have*) oraz metody biometryczne (ang. *Something you are*) [1].

2.1. Metody oparte na wiedzy

Wśród metod opartych na wiedzy użytkownika, jedną z najpopularniejszych jest metoda badająca znajomość (poufnego) hasła przez użytkownika. Hasło należy rozumieć jako ciąg znaków, wybranych przez użytkownika z pewnego alfabetu hasła. Poziom bezpieczeństwa jest proporcjonalny do liczby znaków w alfabecie hasła, ponieważ właśnie od mocy alfabetu (n) oraz długości hasła (l) zależy złożoność ataku metodą brutalną (przeglądu zupełnego) – liczba możliwych haseł to n^l. W celu zmniejszenia skutków ujawnienia hasła stosuje się skracanie okresu jego ważności. Wydaje się, iż najbardziej efektywnym sposobem pozwalającym zminimalizować niebezpieczeństwo, jest stosowanie systemu haseł jednorazowych. Hasła jednorazowe mogą być generowane przez użytkownika bądź przez generator w sposób manualny lub automatyczny. W zakresie przesyłu oraz przechowywania haseł zaleca się korzystanie z łączy komunikacyjnych zabezpieczonych przez podsłuchem, przy czym w czasie transportu, przetwarzania oraz przechowywania hasła powinny być szyfrowane za pomocą jednego z algorytmów, np. RSA czy 3DES. Hasła często przechowywane są w postaci otrzymanej w wyniku przekształcenia jednokierunkową funkcją skrótu. Podwyższenie poziomu bezpieczeństwa przy stosowaniu omawianej metody można uzyskać poprzez tworzenie rejestru historii haseł czy też regularne badania mające na celu wyszukanie haseł łatwych do odgadnięcia. Zasadniczą wadą jest podatność (mimo szyfrowania z użyciem funkcji jednokierunkowych) na ataki słownikowe.

2.2. Metody oparte na materialnych identyfikatorach

Przykładem rozwiązania wykorzystującego metodę opartą na materialnych identyfikatorach jest stosowanie kart identyfikacyjnych. Rolę kart identyfikacyjnych mogą pełnić przykładowo najprostsze w budowie (i najtańsze) karty magnetyczne czy też karty elektroniczne z pamięcią półprzewodnikową. Stosowane są obok kart pamięciowych również karty wyposażone w mikroprocesor (ang. *Smart card*) oraz karty superinteligentne, wyposażone dodatkowo w miniaturowy ekran oraz klawiaturę alfanumeryczną. Karta

elektroniczna cechuje się wysoką odpornością na wpływy pól zewnętrznych (elektromagnetycznego i elektrostatycznego). W czasie realizowanego procesu identyfikacji, informacje zawarte na karcie mogą zostać odczytane za pomocą kontaktowego lub bezkontaktowego czytnika. W ostatnim przypadku transmisja odbywa się przy wykorzystaniu sprzężeń indukcyjnych, fal podczerwonych lub radiowych.

Karty identyfikacyjne stosowane są szeroko w systemach kontroli dostępu do stref i pomieszczeń, w systemach elektronicznych płatności oraz sieciach komputerowych (uzyskanie dostępu do zasobów). Zasadniczą wadą systemów opartych na materialnych identyfikatorach jest możliwość ich zagubienia, kradzieży bądź podrobienia.

2.3. Metody biometryczne

Metody z prezentowanej grupy wykorzystują unikatowość wybranych cech anatomicznych oraz behawioralnych. W procesie weryfikacji/identyfikacji najczęściej badane są wzór tęczówki/siatkówki oka, linie papilarne palców dłoni, kształt dłoni, barwa głosu, sposób pisania na klawiaturze.

W odróżnieniu od procesu identyfikacji, w którym porównanie wyniku następuje z wszystkimi zapamiętanymi wzorcami, częściej w praktyce stosowany jest proces weryfikacji. Proces ten przebiega w podobny sposób jak proces identyfikacji, z tą różnicą, że wynik pomiaru jest porównywany z wzorcem jednego, określonego użytkownika, w tym przypadku potrzebna jest dodatkowa informacja identyfikująca użytkownika, np. nazwa użytkownika. Należy zauważyć, że ze względu na częstą niedokładność wynikającą z charakteru stosowanej metody biometrycznej, czy też natury pomiaru fizycznych cech człowieka, nieodzowne jest stosowanie odpowiednio dobranego zakresu tolerancji dopasowania pomiędzy bieżącym pomiarem a zachowanym wzorcem.

Badanie linii papilarnych jest jedną z metod pozwalających na przeprowadzenie identyfikacji (weryfikacji) tożsamości użytkownika. Pobrany obraz linii papilarnych (przedstawiany dalej w postaci zbioru punktów) jest porównywany z zachowanym wzorcem. Niemożliwe jest przeprowadzenie procesu odwrotnego, tj. w wyniku którego na bazie przechowywanych informacji zostanie wykreowany obraz odcisku palca. Techniki badania linii papilarnych należą do najpopularniej stosowanych z uwagi na niewielki koszt oraz rozmiar urządzenia przeprowadzającego pomiar. W celu jednoznacznego potwierdzenia tożsamości użytkownika wystarczy określić usytuowanie kilkunastu minucji. Istotną wadą jest wpływ stanu powierzchni palca na wynik pomiaru (tj. zabrudzenie, stopień nawilżenia).

3. Wyniki dotychczasowych badań

Dotychczasowe badania wykazały, iż istnieje konieczność dostosowania metody uwierzytelniania do wymagań w zakresie czasu trwania oraz stopnia wiarygodności realizowanego procesu. Zastosowanie metod badających cechy anatomiczne (behawioralne) w celu weryfikacji tożsamości użytkowników pozwala uzyskać poprawę parametrów czasowych oraz jakościowych realizowanego procesu uwierzytelniania w stosunku do pozostałych rodzajów metod uwierzytelniania [2].

Ponadto skłoniły do wyciągnięcia kolejnego wniosku związanego z koniecznością traktowania w sposób kompleksowy systemów uwierzytelniania w trakcie ich oceny, a mianowicie faktu, iż poziom bezpieczeństwa realizowanego procesu uwierzytelniania jest zależny nie tylko od jakości funkcjonowania sprzętowo-programowego systemu biometrycznego, ale również od jakości mechanizmów bezpieczeństwa systemu operacyjnego, w którym jest on implementowany.

Jednym z zaleceń implementacyjnych było odejście od wykorzystania systemów operacyjnych (partykularnie firmy Microsoft), które nie były oparte na jądrze NT (ang. *New Technology*). Przeprowadzona ocena praktycznego zastosowania wybranego rozwiązania (firmy Identicator Technology) obejmowała implementacje jednostanowiskowe, wielostanowiskowe o strukturze równorzędnej, domenowej oraz wielodomenowej. Przedstawiona metodologia oceny wraz z zestawieniem słabych oraz silnych stron stanowiła punkt wyjścia do podjęcia kolejnego etapu prac badawczych, którego celem było przeprowadzenie analizy porównawczej dwóch rozwiązań sprzętowo-programowych różnych producentów, a na podstawie uzyskanych wyników, opracowanie preferencji wykorzystania każdego z nich wraz z zestawieniem właściwości optymalnego biometrycznego systemu uwierzytelniania [2,3].

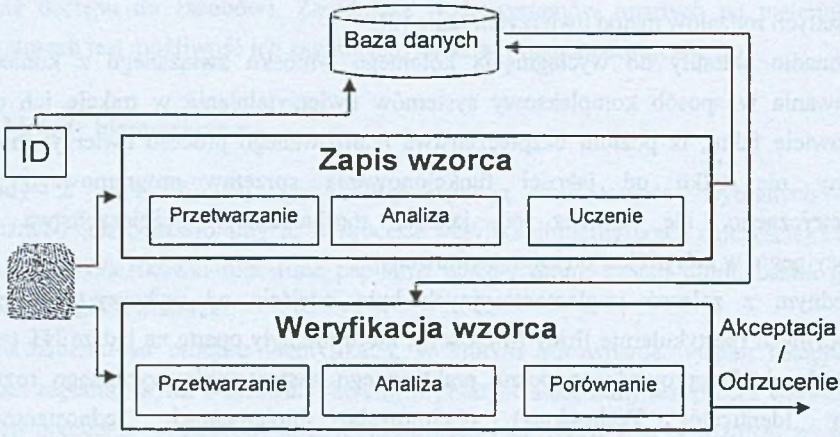
Badania szczegółowych (opartych na wybranej metodzie biometrycznej) realizacji systemów biometrycznych pozwoliły w dalszej kolejności na zbudowanie ogólnego modelu systemu uwierzytelniania oraz określenie charakterystycznych jego parametrów.

4. Model systemu biometrycznego

Każdy system (biometryczny) uwierzytelniania posiada dwa główne moduły: poboru (zapisu) wzorca biometrycznego oraz weryfikacji/identyfikacji. Zapis wzorca do bazy, w systemie pracującym w trybie weryfikacji, wymaga przedłożenia identyfikatora. Dane biometryczne, po wstępnym przetworzeniu, podlegają analizie, w wyniku której

wygenerowywany jest zbiór punktów charakterystycznych (w przypadku linii papilarnych zwanych minucjami), podlegający w dalszym etapie procesowi zapamiętywania (w przypadku weryfikacji mówiącego, tęczówki oka czy też geometrii twarzy – uczenie sieci neuronowej). Analogicznie funkcjonuje drugi moduł, z tą różnicą, iż zamiast procesu uczenia realizowany jest proces porównania wzorca pobranego ze wzorcem referencyjnym.

Ogólny model systemu biometrycznego realizującego proces weryfikacji przedstawiono na rys. 1.



Rys. 1. Ogólny model systemu biometrycznego
Fig. 1. General model of biometric authentication system

Do podstawowych parametrów, które charakteryzują każdy system uwierzytelniania, należą: wskaźnik błędnych odrzuceń (ang. *False Reject Rate*) świadczący o odrzuconych żądaniach uwierzytelniania osoby uprawnionej oraz wskaźnik błędnych akceptacji (ang. *False Accept Rate*) świadczący o przyjętych żądaniach uwierzytelniania osoby nieuprawnionej.

Dodatkowo określa się również parametr błędu siodłowego (ang. *Equal Error Rate*) wyznaczanego na podstawie wskaźników błędnych odrzuceń i akceptacji.

Weryfikacja prawidłowości realizacji składowych zaprezentowanego powyżej modelu, a także rzeczywiste wielkości parametrów charakteryzujących dany system biometryczny mogą zostać osiągnięte jedynie w rezultacie przeprowadzenia praktycznych testów.

Wyniki te stanowią jedynie ilościowy aspekt, który powinien być uzupełniony również o pozostałe czynniki (jakościowe).

5. Implementacja systemu biometrycznego

W dalszej części pracy ostanie zaprezentowany praktyczny przykład konkretnego rozwiązania sprzętowo-programowego służącego do przeprowadzania procesu uwierzytelniania parametryzowanego biometrycznie w środowisku MS Windows 2000. Charakterystyka warstwy sprzętowej i programowej stanowiska badawczego przedstawia się następująco:

1. **Charakterystyka sieci**:
- Typ sieci: klient-serwer
- Ilość serwerów: 1 (S1)
- Ilość stacji roboczych: 2 (K1, K2)
- Administrator domeny (ang. *Domain Administrator*): A_d.
2. **Charakterystyka stacji roboczych** (K1, K2):
- Oprogramowanie: System operacyjny MS Windows 2000 Professional SP2 oraz IDENTIX Biologon Security System v. 2.03 (Client)
- Sprzęt: czytnik linii papilarnych Identix DFR-200
3. **Charakterystyka serwera** (S1):
- Oprogramowanie: System operacyjny MS Windows 2000 Advanced Server SP2 oraz IDENTIX Biologon Security System v. 2.03 (Server)
- Sprzęt: czytnik linii papilarnych Identix DFR-200

Przeprowadzone badania zarówno dla stacji klienckich, jak i serwera wykazały znakomitą adoptowalność systemów biometrycznych w środowisku MS Windows 2000. Głęboka integracja z systemem operacyjnym oraz możliwości dostrojenia systemu biometrycznego stanowią najważniejsze zalety omawianego rozwiązania. Realizacja opracowanych scenariuszy badawczych pozwoliła wysnuć wiele wniosków wynikających z implementacji Identix Biologon Security System v.2.03.

Na silny związek klienta biometrycznego ze środowiskiem systemu operacyjnego wskazały:

- **Integracja z katalogiem aktywnym obiektów systemu.** Spostrzeżenie: integracja z katalogiem aktywnym na drodze modyfikacji schematu domenowego wymaga w pierwszej kolejności ustawienia wartości atrybutu w rejestrze systemowym pozwalającym na modyfikację schematu (zapis), w dalszej części rozbudowę klasy użytkownik oraz z powrotem modyfikację schematu (tylko do odczytu).
- **Integracja narzędzi administracyjnych systemu biometrycznego z narzędziami systemu operacyjnego.** Spostrzeżenie: narzędzia administracyjne systemu biometrycznego są zintegrowane z narzędziami administracyjnymi systemu operacyjnego

(dla kontrolerów domenowych ang. *Active Directory Users and Computers*, dla stacji roboczych ang. *Local Users and Groups*).

O prawdziwości twierdzenia, iż badany system jest konfigurowalny, poświadczyły następujące cechy:

- **Możliwość modyfikacji parametrów procesu poboru wzorca biometrycznego oraz procesu weryfikacji.** Istnieje możliwość modyfikacji wartości progowej, poprzez umowną modyfikację wskaźnika FAR: szczegółowy poziom może być modyfikowany jedynie poprzez wprowadzenie manualnych zmian w rejestrze (HKLM/Software/Identicator Technology/Biologon Security System/BioAuthPackage) odnośnie do wartości progowych w trakcie poboru wzorca (ang. *enrollment*) oraz weryfikacji (ang. *verification*), maksymalnej ilości wzorców do pozostawienia przez jednego użytkownika,
- **Możliwość stworzenia oraz zastosowania reguł bezpiecznego dostępu do systemu.** Istnieje możliwość opracowania oraz aplikacji reguł bezpieczeństwa systemu biometrycznego, ang. *Default biometric policy* (aplikowanej automatycznie po inicjacyjnym procesie poboru wzorca),
- **Możliwość przedłożenia własnej procedury uwierzytelniania użytkownika systemu operacyjnego.** Istnieje możliwość integracji własnej procedury logowania użytkownika z mechanizmami systemu operacyjnego poprzez stosowny wpis w rejestrze wskazujący na własną bibliotekę dynamicznie dołączaną.

Najistotniejsza konkluzja, którą wysnuto w trakcie realizacji badań, związana jest z aspektem bezpiecznego przechowywania wzorców biometrycznych. Zauważono, iż występuje silna zależność poziomu bezpieczeństwa składnicy wzorców od poziomu zabezpieczeń systemu plików. Wzorce biometryczne pozostawione w wewnętrznej bazie systemu operacyjnego (ang. *Security Accunt Manager*) są na tyle silnie strzeżone, na ile pozwala na to system plików (w tym przypadku NTFS v.5.0).

6. Wnioski

Konkurujące ze sobą firmy w przemyśle biometrycznym oferują systemy, które cechuje tendencja do ścisłej integracji z systemem operacyjnym oraz kreowanie szeregu aplikacji pozwalających wykorzystać właściwości biometrycznego hasła, w tym: składnicę haseł (pozwalającą przechować dwójki: nazwa użytkownika oraz hasło), do której dostęp parametryzowany jest biometrycznie, możliwość szyfrowania plików/folderów z poziomu menu kontekstowego czy też kontrolowanej biometrycznie możliwości dostępu do wybranych aplikacji. W dużej mierze są to rozwiązania, których implementacja w środowisku pracy

najczęściej wiążę się z udziałem firm integratorskich bądź też konsultantów (nie stanowią tzw. rozwiązania „*Out of the box*"). Wyniki implementacji w środowisku Microsoft Windows 2000 pozwalają rokować pomyślnie odnośnie do zasadności implementacji w tym środowisku systemu operacyjnego klientów biometrycznych. Kierunkiem dalszych prac będzie próba integracji funkcjonalności różnych metod biometrycznych z własną aplikacją oraz natywnymi mechanizmami uwierzytelniania. W dalszej kolejności zostaną poddane badaniu systemy biometryczne, w celu ustalenia rzeczywistych parametrów ilościowych rozwiązań wybranych producentów.

LITERATURA

1. Kapczyński A.: Biometryczne metody biometryczne uwierzytelniania użytkowników systemów komputerowych. Materiały konferencyjne BISK 2002. PKJS, Bielsko-Biała 2002.
2. Kapczyński A.: Ocena zostosowania wybranej metody biometrycznej w procesie autentykacji. Studia Informatica, Vol. 22, Number 1(43), Gliwice 2001.
3. Kapczyński A.: Analiza porównawcza wybranych biometrycznych rozwiązań sprzętowo-programowych wykorzystujących badanie linii papilarnych w procesie uwierzytelniania. Techniki komputerowe 1/2001, Instytut Maszyn Matematycznych, Warszawa 2001.

Recenzent: Dr inż. Bartłomiej Zieliński

Wpłynęło do Redakcji 25 marca 2002 r.

Abstract

At the beginning three types of authentication methods are described, i.e. based on something one know (e.g. password), something one have (e.g. smart card) or something one is (e.g. fingerprint).

In presented paper implementation of chosen biometric solution based on Microsoft Windows 2000 operating system environment, namely Biologon Security System v.2.03 was discussed. In explored case biometrics system seamlessly integrates biometrics data with Windows 2000 security model.

Installed biometrics system is closely integrated and dependent on operating system installed on given computer. On the assumption that security issue is the most significant matter, choosing that environment is highly recommended and estimated positively. In a networked client/server architecture administrative tools let one easily configure security settings (workstation policy, smart card policy, default biometric policy for local workstation and domain controller). Biologon 2.03 server can be integrated with Microsoft Active Directory with previous addition of attribute "idx-Biologon-BioID0" to the user class in domain schema. In order to perform schema update specific values in the registry should be entered. To sum up presented biometrics solution provides more benefits than utilization of classic methods, such as logon using password or smart card.