STUDIA INFORMATICA 2001
Volume 22 Number 1 (43)

Adrian KAPCZYŃSKI
Politechnika Śląska, Katedra Informatyki i Ekonometrii

OCENA ZASTOSOWANIA WYBRANEJ METODY BIOMETRYCZNEJ W PROCESIE AUTENTYKACJI UŻYTKOWNIKÓW

Streszczenie. W niniejszym artykule przedstawiono metodę biometryczną wykorzystującą odciski palców w celu przeprowadzenia autentykacji użytkowników. W pracy zaprezentowano oraz oceniono rozwiązania oparte na Biologon Security System v. 2.0 firmy IDENTIX, implementowane w systemach operacyjnych rodziny Microsoft Windows, z wykorzystaniem klawiatury firmy CHERRY GMBH model G81-12000 z zintegrowanym czytnikiem linii papilarnych.

ESTIMATION OF APPLICATION OF A CHOSEN BIOMETRIC METHOD IN THE USER'S AUTHENTICATION PROCESS

Summary. In presented paper biometrics method using fingerprints in authentication process was described. Moreover Author provided characteristics and estimation of implementation of IDENTIX Biologon Security System v. 2.0 in Microsoft Windows environment basing on CHERRY GMBH model G81-12000 with integrated fingerprint reader.

1. Wprowadzenie

Dynamiczny rozwój technologiczny, zwłaszcza techniki komputerowej, stworzył możliwość szybkiej analizy ogromnych ilości informacji dotyczących dowolnych obszarów otoczenia. Podstawowym środkiem pozwalającym zaspokoić potrzeby informacyjne użytkowników systemów komputerowych jest system informatyczny, składający się z następujących elementów: sprzęt, oprogramowanie, baza danych, telekomunikacja, ludzie, organizacja.

Do podstawowych zadań realizowanych przez system informatyczny funkcjonujący w obiektach gospodarczych należą między innymi: usprawnienie przebiegu procesów zrutynizowanych, wykonywanych wg stałych procedur, usprawnienie procesu podejmowania decyzji poprzez dostarczanie wiarygodnej informacji w stosownym czasie, umożliwienie dzielenia się zasobami informacyjnymi.

System informatyczny, aby móc realizować wymienione zadania w sposób zadowalający, powinien spełniać stawiane mu wymagania, które mogą się zmieniać w zależności od potrzeb użytkownika(ów). Do najważniejszych kryteriów, które powinny być spełnione przez system informatyczny, należą:

- niezawodność (ang. *reliability*),
- funkcjonalność (ang. *functionality*),
- wydajność (ang. *performance*),
- efektywność (ang. *efficiency*),
- elastyczność (ang. *flexibility*),
- bezpieczeństwo (ang. *security*).

Ostatnie z wymienionych kryteriów, tj. bezpieczeństwo, jest szczególnie istotne z punktu widzenia poprawności działania całego systemu komputerowego. Informacja, która jest przetwarzana w systemach, nie może być narażona na zniszczenie i zmiany przez osoby niepowołane.

2. Bezpieczeństwo systemów komputerowych

Z uwagi na powszechność stosowania komputerów oraz sieci teleinformatycznych, a także ze względu na ilość oraz znaczenie przechowywanej informacji w każdym z obiektów gospodarczych pojawia się konieczność ciągłego zabezpieczania systemów komputerowych.

W celu zapewnienia bezpieczeństwa systemów stosowanych jest wiele metod i środków ochrony.

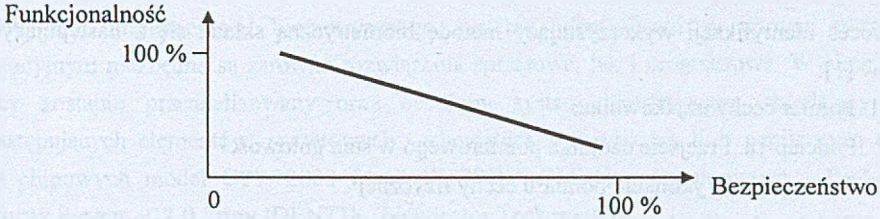
Wśród wybranych metod ochrony można wyróżnić następujące:

- ochrona przed wpływem czynników zewnętrznych,
- ochrona dostępu do pomieszczeń,
- ograniczanie uprawnień użytkowników,
- kryptografia,
- audyt,
- redundancja sprzętu,
- ochrona antywirusowa,
- zapewnienie ciągłości zasilania,

- **identyfikacja i uwierzytelnianie użytkowników.**

Stosowanie jednocześnie wszystkich (wyżej wymienionych i nie tylko) mechanizmów bezpieczeństwa w danym obiekcie gospodarczym nie jest w stanie zlikwidować całkowicie potencjalnych zagrożeń.

Należy zauważyć, że wzrost poziomu bezpieczeństwa jest zwykle uzyskiwany kosztem spadku funkcjonalności oraz efektywności systemu (rys. 1).



Rys. 1. Zależność między funkcjonalnością a bezpieczeństwem systemu
Fig. 1. Dependency between system functionality and security

Część ze stosowanych metod zabezpieczeń jest ściśle powiązana z oprogramowaniem systemowym oraz aplikacjami (identyfikacja, ograniczanie uprawnień), a część jest od nich niezależna (np. ochrona antywirusowa).

W dalszej części artykułu zostaną rozpatrzone wyróżnione powyżej metody autentykacji użytkowników systemów komputerowych.

3. Metody autentykacji użytkowników

Wśród metod służących do autentykacji użytkowników wyróżnia się:

- metody oparte na wiedzy użytkowników (np. hasła),
- metody oparte na materialnych identyfikatorach (np. karty chipowe),
- metody biometryczne.

Metody z ostatniej z wymienionych grup wykorzystują unikatowość wybranych charakterystyk fizycznych człowieka oraz jego zachowań.

W procesie identyfikacji najczęściej badane są: linie papilarne palców dłoni, kształt dłoni, głos, wzór tęczówki oka, sposób pisania na klawiaturze. Przykłady rozwiązań (opartych na badaniach określonej cechy) oferowanych przez wybranych producentów zostały przedstawione w tabeli 1.

Tabela 1

Przykłady rozwiązań biometrycznych

Cecha	Nazwa	Firma	Cena [zł]
Głos	BIOID	DCS AG	300
Linie papilarne	Secure Touch	Biometric Access Corp.	2000
Dłoń	Handkey II	Recognition Systems, Inc.	10000

Proces identyfikacji wykorzystujący metodę biometryczną składa się z następujących etapów [1]:

Etap 1. Pomiar cechy użytkownika:

- Podetap 1a. Przejście czujnika pomiarowego w stan gotowości
- Podetap 1b. Wykonanie pomiaru cechy fizycznej
- Podetap 1c. Przekazanie do systemu sygnałów cyfrowych reprezentujących wynik pomiaru

Etap 2. Porównanie wyniku pomiaru z zachowanymi wzorcami

W odróżnieniu od procesu identyfikacji, w którym porównanie wyniku następuje z wszystkimi zapamiętanymi wzorcami (patrz etap 2), częściej w praktyce stosowany jest proces weryfikacji. Proces ten przebiega w analogiczny sposób jak proces identyfikacji, z tą jednak różnicą, że wynik pomiaru jest porównywany ze wzorcem jednego, określonego użytkownika. W tym przypadku potrzebna jest dodatkowa informacja identyfikująca użytkownika – identyfikator, nazwa użytkownika (ang. *username*).

Należy zauważyć, że ze względu na częstą niedokładność wynikającą z charakteru stosowanej metody biometrycznej, czy też natury pomiaru fizycznych cech człowieka, nieodzownem jest stosowanie odpowiednio dobranego zakresu tolerancji dopasowania pomiędzy bieżącym pomiarem a zachowanym wzorcem.

W omawianym zagadnieniu istotna jest analiza dwóch wskaźników, których wielkości zmieniają się wraz ze zmianą zakresu tolerancji. Należą do nich: wskaźnik błędnych odrzuceń (FRR – ang. *False Reject Rate*), świadczący o odrzuconych autentykacjach osoby uprawnionej oraz wskaźnik błędnych akceptacji (FAR - ang. *False Accept Rate*), świadczący o przyjętych autentykacjach osoby nieuprawnionej.

Im wyższy zakres tolerancji, tym bardziej system będzie przyjazny dla użytkownika (niższy FRR); równocześnie zwiększy się ryzyko akceptowania nieautoryzowanych użytkowników (wyższy FAR).

W obszarze zainteresowań niniejszego artykułu leży metoda biometryczna, badająca odciski palców i na tej podstawie weryfikująca tożsamość użytkowników. 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. Należy nadmienić, iż dany system nie może przeprowadzić procesu odwrotnego, tzn. takiego, w wyniku którego na bazie przechowywanych informacji zostanie wykreowany obraz odcisku palca.

4. Zastosowanie wybranej metody w praktyce

W celu implementacji biometrycznego systemu identyfikacji w danym systemie operacyjnym niezbędne są zarówno rozwiązania sprzętowe, jak i programowe. W niniejszej pracy zostanie przeanalizowany oraz oceniony system biometryczny składający się z następujących elementów: sprzętowych - klawiatura z czytnikiem linii papilarnych oraz kart chipowych model G81-12000 firmy CHERRY GMBH; programowych - Biologon Security System v. 2.0 firmy IDENTIX (Identicator Technology).

4.1. Charakterystyka elementów analizowanego rozwiązania

IDENTIX Biologon Security System v. 2.0 jest rozwiązaniem przeznaczonym dla środowisk systemów operacyjnych firmy Microsoft: MS Windows 95/98 (wraz Internet Explorer v. 3.02 lub nowszym), MS Windows NT Workstation 4.0 (wraz z Service Pack 3 lub wyższym), MS Windows NT Server 4.0 (wraz z Service Pack 3 lub wyższym) [2].

Prezentacja konkretnych implementacji omawianego produktu zostanie poprzedzona przedstawieniem minimalnych wymagań niezbędnych do instalacji oraz użytkowania Biologon Security System v. 2.0 (tabela 2).

Tabela 2

Najważniejsze wymagania sprzętowe badanego rozwiązania

Komponent	Wymagania
Procesor	486/33DX lub szybszy
Pamięć RAM	16 MB (32 zalecane)
Wolna przestrzeń dysku twardego	10 MB
Port równoległy	dostępny[1]
Port szeregowy	dostępny[2]
Stacja CD-ROM	dostępna[3]
Interfejs sieciowy	dostępny[4]

[1] Wymagany przez czytnik linii papilarnych
[2] Wymagany przez czytnik kart chipowych
[3] Stacja CD-ROM nie jest wymagana w przypadku instalacji z sieci.
[4] Interfejs sieciowy nie jest wymagany w przypadku implementacji w wolno stojącej maszynie (rozwiązanie indywidualne).

W pracy postanowiono poddać ocenie implementacje, w których z założenia systemy identyfikacji biometrycznej wykorzystują wyłącznie wbudowany w klawiaturę czytnik linii papilarnych FPR 12000 (niewykorzystywany jest czytnik kart chipowych).

4.2. Przykłady rozwiązań opartych na IDENTIX Biologon Security System v. 2.0

W niniejszej części artykułu zostanie przedstawiona charakterystyka oraz ocena zastosowania indywidualnego badanego systemu autentykacji, zastosowania w sieci o strukturze grupy roboczej oraz w sieci o strukturze domeny.

4.2.1. Charakterystyka oraz ocena zastosowania indywidualnego

Przed przystąpieniem do analizy efektów indywidualnego zastosowania systemu biometrycznego zostanie opisany proces instalacji, konfiguracji oraz użytkowania IDENTIX Biologon Security System v. 2.0.

4.2.1.1. Instalacja, konfiguracja oraz użytkowanie systemu

System biometryczny w analizowanej konfiguracji będzie implementowany zgodnie z przedstawionymi poniżej założeniami:

a) Charakterystyka systemu:
   i) Ilość stacji roboczych: 1 (Stacja1),
   ii) Użytkownicy:
      (1) A - Administrator stacji roboczej
      (2) U_j- j-ty użytkownik stacji roboczej, gdzie: j=1,2

b) Charakterystyka stacji roboczej:
   i) Oprogramowanie:
      (1) System operacyjny: MS Windows 95 (MS Windows 98)
      (2) IDENTIX Biologon Security System v. 2.0
   ii) Specyfikacja urządzenia wejścia: klawiatura CHERRY GMBH G81-12000
   iii) Brak interfejsu sieciowego
   iv) Stanowisko pracy: wieloosobowe.

W dalszej części zostanie zaprezentowany opis etapów **instalacji, uruchomienia, konfiguracji oraz użytkowania** systemu biometrycznego.

Etap 1. Instalacja oprogramowania oraz sprzętu do identyfikacji biometrycznej

1) W zakładanej strukturze systemu występuje jedna stacja robocza, zatem w celu zaimplementowania systemu identyfikacji opartego na metodzie biometrycznej należy jednokrotnie zrealizować procedurę instalacji klawiatury CHERRY GMBH G81-12000 oraz oprogramowania IDENTIX Biologon Security System v. 2.0. Procedura instalacji oprogramowania IDENTIX Biologon Security System v. 2.0 w systemie Microsoft

Windows 95/98[5] związana jest z wyborem użytkownika, któremu zostaną przydzielone prawa Administratora[6]. Istnieje możliwość wyboru jednego z zarejestrowanych użytkowników w systemie bądź też stworzenie nowego konta użytkownika. W dalszej kolejności ma miejsce uruchomienie kreatora poboru wzorca biometrycznego Administratora:

- skanowanie odcisku wybranego palca[7],
- weryfikacja (powtórne skanowanie odcisku wybranego palca oraz porównanie z wzorcem pobranym wcześniej).

Etap 2. Uruchomienie systemu

Po zakończonym etapie instalacji oprogramowania użytkownik pełniący funkcję Administratora może zostać zidentyfikowany w systemie poprzez:

- podanie *Nazwy użytkownika* oraz hasła,
- podanie *Nazwy użytkownika* oraz dostarczenie odcisku palca,
- podanie PIN-u oraz dostarczenie karty chipowej.

Domyślnie, po instalacji opisywanego oprogramowania wszystkie z wymienionych metod logowania się są dostępne. Z rozwijanego menu, oprócz możliwości wyboru metody logowania, można dostroić czytnik linii papilarnych oraz przeprowadzić test poprawności zainstalowanych komponentów systemu Biologon Security System v. 2.0.

Etap 3. Konfiguracja oraz administracja systemem

Użytkownik pełniący funkcję Administratora za pomocą *Biologon Security*[8] (zakładka *Security*) może ustalić dostępność metod logowania z menu okna logowania do systemu (grupa opcji *Workstation Policy*). Ponadto z poziomu grupy opcji *Security level* może być konfigurowana wielkość wskaźnika błędnych akceptacji (FAR), mogącego przyjąć jedną z trzech wartości: 1/1000 (średni poziom), 1/10000 (wysoki poziom), 1/100000+ (bardzo wysoki poziom).

Istnieje również możliwość zapisu zdarzeń do pliku log na jednym z trzech poziomów szczegółowości: standardowym, szczegółowym, pełnym.

Administrator posiada możliwość operowania na kontach użytkowników. Instalacja IDENTIX Biologon Security System v. 2.0 wprowadza modyfikacje do komponentu *Użytkownicy*, wchodzącego w skład Panelu sterowania (USERS.CPL). Okno wspomnianego komponentu zostało wzbogacone o przycisk "*Biometrics*".

---

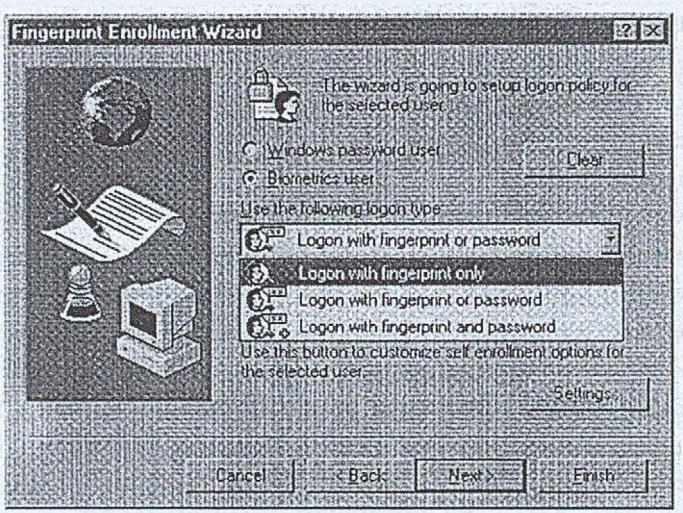
[5] Procedura instalacji w systemie MS Windows NT Workstation 4.0 oraz MS Windows NT Server 4.0 przebiega w sposób zbliżony (pominięcie pkt. 3 w Kroku 4).

[6] Instalacja Biologon Security System v. 2.0 w przypadku systemu MS Windows NT Workstation 4.0 lub MS Windows NT Server 4.0 jest realizowana przez Administratora.

[7] Możliwe jest zachowanie więcej niż jednego wzorca biometrycznego dla jednego użytkownika.

[8] Doinstalowany komponent Panelu sterowania

Dla każdego konta Administrator może określić, czy użytkownik jest "użytkownikiem biometrycznym" (ang. *Biometrics User*), czy też pozostaje "użytkownikiem niebiometrycznym" (ang. *Windows password user*) – patrz rys. 2.



Rys. 2. Okno modyfikacji rodzaju konta
Fig. 2. Modification Window of logon policy

Zaliczenie danego użytkownika do grupy użytkowników biometrycznych pozwala na sprecyzowanie typu logowania (ang. *Logon type*):

Typ 1. Wyłącznie odcisk palca

Typ 2. Odcisk palca lub hasło

Typ 3. Odcisk palca i hasło

Kolejnym etapem jest pobranie wzorców biometrycznych oraz skojarzenie ich z użytkownikiem (ang. *enrollment*). W kwestii procedury poboru wzorców biometrycznych, Administator ma prawo:

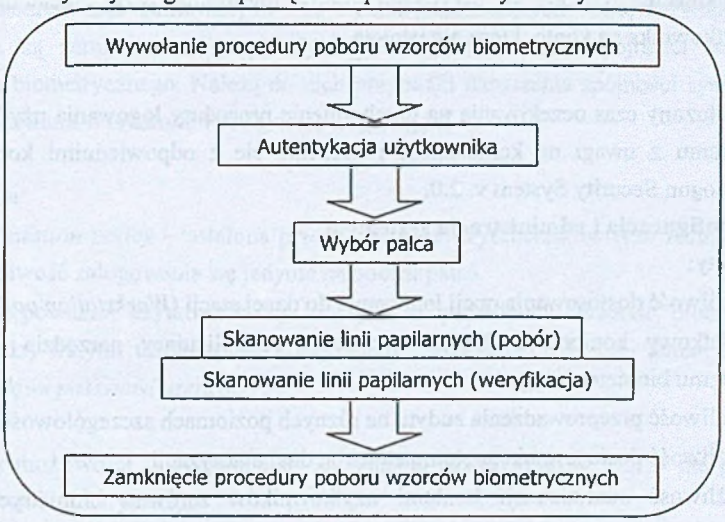
- nakazać pobór wzorców biometrycznych przy następnym logowaniu użytkownika,
- pozostawić decyzję o momencie poboru wzorców użytkownikowi,
- zabronić samodzielnego przeprowadzania procedury poboru wzorców (ang. *self enrollment*) tym samym zezwalając użytkownikowi na skanowanie linii papilanych jedynie wtedy, gdy Administrator uruchomi stosowną procedurę ze swojego konta.

Etap 4. Użytkowanie systemu

W przypadku Microsoft Windows 95/98 instalacja Biologon Security System v. 2.0 podniosła bezpieczeństwo systemu poprzez wprowadzenie wybranych rozwiązań stosowanych w przypadku systemu(ów) Microsoft Windows NT.

Za przykład może posłużyć okno bezpieczeństwa (ang. *Windows Security*) uruchamiane poprzez naciśnięcie klawiszy CTRL+ALT+DELETE, pozwalające (podobnie jak użytkownikom systemów rodziny Microsoft Windows NT) dokonać następujących operacji: Zamknij system, Uruchom menedżer zadań, Zmień hasło, Zablokuj stację[9].

Użytkownik, po zalogowaniu na swoje konto w tradycyjny sposób (hasło), posiada (o ile Administrator tego nie zabronił) możliwość przeprowadzenia procedury poboru przez system wzorców biometrycznych zgodnie porządkiem przedstawionym na rys. 3.



Rys. 3. Procedura poboru wzorców biometrycznych
Fig. 3. Procedure of conscription of biometric templates

4.2.1.2. Ocena zastosowania indywidualnego

W celu oceny rozwiązań indywidualnych zostaną przeanalizowane etapy związane z wdrożeniem systemu identyfikacji biometrycznej.

Etap 1. Instalacja oprogramowania oraz sprzętu do identyfikacji biometrycznej

1. Zalety:
   - szybki, nieskomplikowany proces instalacji, realizowany za pomocą kreatora,
   - wymagana stosunkowo niewielka ilość wolnego miejsca na twardym dysku.
2. Wady:
   - konieczność zapewnienia niezajętego portu równoległego,
   - funkcjonowanie wyłącznie w środowiskach systemowych firmy Microsoft.

Etap 2. Uruchomienie systemu

[9] Zamiast polecenia „Wyloguj" zostało wprowadzone polecenie pobrania wzorców biometrycznych przez system.

1. Zalety:
   - testy diagnostyczne czytnika linii papilarnych po uruchomieniu systemu,
   - możliwość przeprowadzenia dodatkowych testów diagnostycznych FPR 12000,
   - możliwość dostrojenia przed zalogowaniem czytnika linii papilarnych,
   - możliwość wyboru z menu sposobu logowania (aktywne w menu metody logowania określane są przez parametr *Workstation policy*),
   - zamknięcie systemu w przypadku próby logowania przez nieautoryzowanego użytkownika na konto, które nie istnieje.
2. Wady:
   - wydłużony czas oczekiwania na uruchomienie procedury logowania użytkownika do systemu z uwagi na konieczność połączenia się z odpowiednimi komponentami Biologon Security System v. 2.0.

Etap 3. Konfiguracja i administracja systemem

1. Zalety:
   - możliwość dostosowania opcji logowania do danej stacji (*Workstation policy*),
   - dodatkowy komponent Panelu sterowania centralizujący narzędzia konfiguracji systemu biometrycznego,
   - możliwość przeprowadzenia audytu na różnych poziomach szczegółowości,
   - możliwość dostosowania poziomu stopy błędnej autoryzacji,
   - możliwość administracji kontami użytkowników zarówno biometrycznych, jak i niebiometrycznych z poziomu komponentu „Użytkownicy" (dzięki modyfikacji tego składnika – dodanie przycisku polecenia „*Biometrics*"),
   - możliwość ustalenia dla każdego z użytkowników z osobna, indywidualnie (ang. *per user*) sposobu logowania (ang. *logon type*).
2. Wady:
   - wszyscy użytkownicy (biometryczni oraz niebiometryczni) posiadają możliwość ustalenia właściwości mechanizmu bezpieczeństwa (akceptowane sposoby logowania, rodzaj audytu, poziom stopy błędnej autoryzacji) obowiązujące dla wszystkich użytkowników danej stacji roboczej,
   - potencjalne zagrożenie naruszenia spójności funkcjonowania systemu.

Etap 4. Użytkowanie systemu

1. Zalety:
   - szybki proces logowania,
   - możliwość stosowania więcej niż jednej metody autentykacji,
   - implementacja wybranych elementów rozwiązań bezpieczeństwa zastosowanych w MS Windows NT,

- możliwość przeprowadzenia procedury poboru wzorców biometrycznych przez użytkownika,
- szybka, nieskomplikowana procedura poboru wzorców biometrycznych.

2. Wady:
   - słabe zabezpieczenie przechowywanych wzorców biometrycznych

4.2.1.3. Przykłady naruszenia spójności systemu biometrycznego

Uzupełnieniem zaprezentowanych wad i zalet, kształtujących ocenę rozwiązania indywidualnego, są zamieszczone przykłady możliwości naruszenia spójności omawianego rozwiązania biometrycznego. Należą do nich przypadki naruszenia spójności systemu związane z parametrami *Workstation policy* oraz *Logon type*.

Przykład 1

1. Założenia:
   - *Workstation policy* – ustalona przez jednego z użytkowników (lub Administratora): możliwość zalogowania się jedynie na odcisk palca.
   - Występowanie użytkowników, którzy nie pozostawili wzorca biometrycznego (między innymi użytkownicy korzystający z tradycyjnej metody autentykacji (ang. *Windows password users*)).
2. Rezultat:
   - Brak możliwości zalogowania się do systemu użytkowników, którzy nie pozostawili wzorca biometrycznego.

Przykład 2

1. Założenia:
   - *Workstation policy* – ustalona przez jednego z użytkowników (lub Administratora): możliwość zalogowania się na odcisk palca lub hasło.
   - Występowanie użytkowników, którzy nie pozostawili wzorca biometrycznego (między innymi użytkownicy korzystający z tradycyjnej metody identyfikacji.
   - Po zalogowaniu (na hasło) zmiana *Workstation policy* na możliwość zalogowania się jedynie na odcisk palca.
2. Rezultat:
   - Po zablokowaniu stacji występuje brak możliwości zmiany wartości w polu *Username* (np. na Administratora).
   - Po zablokowaniu stacji występuje brak możliwości odblokowania stacji przez użytkownika (konieczność zrestrartowania systemu).

Przykład 3

1. Założenia:
   - Administrator posiada ustawienie *Logon type* na: wyłącznie odcisk palca oraz ustanawia *Workstation policy* na możliwość zalogowania się jedynie na odcisk palca.

- *Workstation policy* – zostaje ustalona przez jednego z użytkowników na możliwość zalogowania się jedynie na hasło.

2. Rezultat:
   - Administrator nie ma możliwości przedłożenia w celu weryfikacji odcisku palca (czytnik nieaktywny).
   - Administrator ma możliwość przedłożenia hasła w celu autentykacji, jednakże ta metoda logowania nie pozwoli na zalogowanie się (z uwagi na przyjęty typ logowania).

Przyczyna ww. nieprawidłowości:

- możliwość ustalenia obowiązującej wszystkich użytkowników (włączając Administratora) *Workstation policy* przez dowolnego użytkownika, niezgodnej z polityką opracowaną przez Administratora.

Zestawienie ustawień parametrów *Workstation policy* oraz *Logon type* wraz z określeniem, czy występuje konflikt, prezentuje tabela 3.

Tabela 3

Zestawienie ustawień parametrów bezpieczeństwa systemu

		Workstation policy		*Blokada*
		ODCISK PALCA	HASŁO	(konflikt)
Logon Type	Wyłącznie odcisk palca	N	T	TAK
	odcisk palca lub hasło	N	T	NIE
		T	N	
	odcisk palca i hasło	N	T	TAK
		T	N	
	brak (Wyłącznie hasło)	T	N	TAK

W dalszej części pracy zostanie rozpatrzona sytuacja zagrożenia przechowywanych wzorców biometrycznych w stacjach roboczych.

W analizowanym rozwiązaniu występuje ryzyko naruszenia spójności omawianego mechanizmu bezpieczeństwa z uwagi na **niewłaściwe zabezpieczenie składnicy pobranych wzorców biometrycznych użytkowników** poszczególnych stacji roboczych.

W każdej ze stacji roboczych pobrane wzorce biometryczne przechowywane są w rejestrze systemowym. Przykładowy fragment rejestru systemu:

Rejestr systemowy:

[HKEY_LOCAL_MACHINE\Software\Identicator Technology\Biologon Security System\BioAccountManager\Database\A]

BioID [01, 02, 01, 03, 05, 02, 09...]

BioProp [02,02,02,03,02,04,02,...]

[HKEY_LOCAL_MACHINE\Software\Identicator Technology\Biologon Security System\BioAccountManager\Database\U1]

BioID [04, 09, 02, 01, 06, 06, 08...]

[HKEY_LOCAL_MACHINE\Software\Identicator Technology\Biologon Security System\BioAccountManager\Database\U2]

BioID [07, 09, 04, 02, 02, 05, 01...]

Przyjmując, iż U2 jest Napastnikiem, dla wybranej stacji roboczej może zaistnieć przykładowo następująca sytuacja zagrożenia:

1. **Założenia:**
   - *Workstation policy* – możliwość logowania: hasło, odcisk palca
   - *Logon type* – akceptowany sposób logowania na konto U1, U2: hasło lub odcisk palca (ang. *Password or fingerprint)*
2. **Procedura ataku:**

2.1. Zalogowanie Napastnika na konto U2

2.2. Uruchomienie aplikacji **Regedit.exe**

2.3. Odnalezienie gałęzi:

HKEY_LOCAL_MACHINE/Software/Identicator Technology/Biologon SecuritySystem/BioAccountManager/Database/

2.4. Zmiana nazw kluczy U1 i U2 w podanej powyżej lokalizacji:
- ... Database/U1 --- Zmiana nazwy ---> ... Database/U1a
- ... Database/U2 --- Zmiana nazwy ---> ... Database/U1
- ... Database/U1a --- Zmiana nazwy ---> ...Database/U2

2.5. Uruchomienie procedury poboru odcisku palca użytkownika U2:
- Autoryzacja użytkownika U2 przez podanie hasła
- Pobór i zapisanie wzorca biometrycznego

2.6. Ponowne uruchomienie aplikacji **Regedit.exe**

2.7. Ponowna zmiana nazw kluczy U1 i U2:
- ... Database/U1 --- Zmiana nazwy ---> ... Database/U1a
- ... Database/U2 --- Zmiana nazwy ---> ... Database/U1
- ... Database/U1a --- Zmiana nazwy ---> ... Database/U2

2.8. Wylogowanie Napastnika

2.9. Zalogowanie Napastnika na konto U1 (z wykorzystaniem pozostawionego wzorca biometrycznego (punkt e))

2.10. Dodatkowe działania:

- Możliwość podmiany/usunięcia wzorca biometrycznego pozostawionego przez użytkownika U1.
- Możliwość zmiany hasła ustanowionego przez U1 (pod warunkiem ustawienia weryfikacji tożsamości na sprawdzenie odcisku palca, co ozn. usunięcie pola przeznaczonego na wpis starego hasła (ang. *old password*)).

2.11. Zakończenie ataku, powrót do stanu pierwotnego:

- Usunięcie wzorca biometrycznego pozostawionego przez Napastnika w punkcie e.

Zaprezentowana procedura ataku jest dowodem na brak właściwego mechanizmu zabezpieczającego przechowywane wzorce biometryczne. Jakość bezpieczeństwa całego systemu zależy od jakości mechanizmów zainstalowanego oprogramowania, a także jakości mechanizmów bezpieczeństwa zaimplementowanych w systemie operacyjnym, w którym Biologon Security System v. 2.0 jest zainstalowany.

Korzystanie z wymienionego wcześniej programu, pozwalającego na wprowadzanie zmian w rejestrze systemu, umożliwia Napastnikowi usunięcie klucza wybranego użytkownika – następuje wówczas utrata pozostawionych wzorców biometrycznych, przemianowanie na standardowego użytkownika systemu (*Windows password user*).

W obliczu przedstawionych wad i zalet niniejsze zastosowanie oceniono negatywnie, nie zalecając stosowania.

4.2.2. Charakterystyka oraz ocena zastosowania w sieci o strukturze grupy roboczej

System biometryczny w analizowanej konfiguracji będzie implementowany zgodnie z przedstawionymi poniżej założeniami:

a)Charakterystyka sieci:

i) Typ sieci: każdy-z-każdym

ii) Ilość stacji roboczych: 4 (Stacja1, ... , Stacja4)

iii) Użytkownicy:

(1) A_i - Administrator i-tej stacji roboczej, gdzie: $A_i=A_{i+1}$, dla i=1,2,3

(2) U_{ij}- j-ty użytkownik i-tej stacji roboczej, gdzie: j=1,2, i=1,2,3,4

b)Charakterystyka stacji roboczej [10]:

i) Oprogramowanie:

(1) System operacyjny: MS Windows 98

(2) IDENTIX Biologon Security System v. 2.0

ii) Specyfikacja urządzenia wejścia: klawiatura CHERRY GMBH G81-12000.

W przypadku prezentowanej struktury sieci występują dodatkowe możliwości w porównaniu do rozwiązania indywidualnego. Należy do nich możliwość instalacji Biologon Security System poprzez sieć, tj. z maszyny, w której zlokalizowana jest wersja

[10] Stacje robocze posiadają takie same charakterystyki.

instalacyjna wspomnianego programu. Eliminuje to konieczność instalacji wykorzystujących czytniki płyt kompaktowych zainstalowanych w każdej ze stacji roboczych.

W zasadzie rozwiązanie obejmujące implementację Biologon Security System w strukturze grupy roboczej (sieć typu każdy-z-każdym) w dużej mierze jest zbliżone do rozwiązania indywidualnego.

Niestety, nie występuje możliwość zdalnego zarządzania systemami biometrycznymi poszczególnych stacji przez osobę pełniącą funkcję Administratora.

Podobnie jak i w przypadku rozwiązania indywidualnego występuje ryzyko naruszenia integralności mechanizmu bezpieczeństwa związanego z identyfikacją użytkowników. Zachodzi analogiczna sytuacja jak w przypadku rozwiązania indywidualnego, gdzie słabości systemu były powodowane brakiem mechanizmu zezwalającego na ustawienie opcji bezpieczeństwa jedynie osobie pełniącej funkcję Administratora.

Na podstawie przedstawionej charakterystyki niniejsze zastosowanie oceniono negatywnie, nie zalecając stosowania.

4.2.3. Charakterystyka oraz ocena zastosowania w sieci o strukturze domeny

System biometryczny w analizowanej konfiguracji będzie implementowany zgodnie z przedstawionymi poniżej założeniami:

a) Charakterystyka sieci:
   i) Typ sieci: klient-serwer
   ii) Ilość serwerów: 1 (Serwer1)
   iii) Ilość stacji roboczych: 2 (Stacja1, Stacja2)
   iv) Nazwa domeny: TEST
   v) Administrator domeny (ang. *Domain Administrator*): A_d
b) Charakterystyka stacji roboczej[11]:
   i) Oprogramowanie:
      (1) System operacyjny: Stacja 1 - MS Windows 98, Stacja 2 - MS Windows NT Workstation 4.0
      (2) IDENTIX Biologon Security System v. 2.0
   ii) Specyfikacja urządzenia wejścia: klawiatura CHERRY GMBH G81-12000
   iii) Użytkownicy:
      (1) A_i - Administrator i-tej stacji roboczej, gdzie: $A_i=A_d$, dla i=2
      (2) U_{ij}- j-ty użytkownik i-tej stacji roboczej, gdzie: j=1,2, i=1,2.
c) Charakterystyka serwera:
   i) Oprogramowanie:
      (1) System operacyjny: MS Windows NT Server 4.0

[11] Stacje robcze posiadają takie same charakterystyki.

(2) IDENTIX Biologon Security System v. 2.0

ii) Specyfikacja urządzenia wejścia: klawiatura CHERRY GMBH G81-12000

iii) Użytkownicy:

(1) A_d - Administrator domeny.

W niniejszej konfiguracji systemu występują dwie stacje robocze. Jedna z nich funkcjonuje w oparciu o system operacyjny MS Windows NT Workstation 4.0, którego wbudowane mechanizmy i procedury bezpieczeństwa są silniejsze od występujących w systemie MS Windows 98, zainstalowanym na drugiej stacji roboczej.

Omawiana struktura sieci charakteryzuje się występowaniem komputera pełniącego funkcję serwera, co stanowi podstawę rozwiązania wykorzystującego domenę.

Zastosowanie systemu MS Windows NT Workstation 4.0 na jednej ze stacji roboczych pozwoliło wyeliminować zaprezentowane wcześniej możliwości naruszenia spójności systemu bezpieczeństwa, a w szczególności:

- wyłącznie Administrator posiada możliwość ustalenia właściwości mechanizmu bezpieczeństwa (akceptowane sposoby logowania, rodzaj audytu, poziom stopy błędnej autoryzacji) obowiązujące dla wszystkich użytkowników danej stacji roboczej,
- nie występuje potencjalne zagrożenie naruszenia spójności funkcjonowania systemu, związane z parametrami *Workstation policy* oraz *Logon type* (przykłady: 1,2 i 3),
- występuje właściwe zabezpieczenie składnicy pobranych wzorców biometrycznych użytkowników (niemożliwe jest zrealizowanie zaprezentowanej wcześniej procedury ataku).

W przypadku „Stacja1" (z systemem operacyjnym MS Windows 98) w celu przystosowania do pracy w domenie należy:

- ustawić nazwę grupy roboczej „Stacja1", taką samą jak nazwa domeny,
- ustanowić weryfikację logowania w domenie o nazwie TEST (właściwości klienta sieci MS Networks),
- ustanowić kontrolę dostępu na poziomie użytkownika, wskazując źródło listy użytkowników z domeny o nazwie TEST,
- zezwolić na zdalną administrację systemem (Administratorowi domeny).

W przypadku „Stacja2" należy przeprowadzić procedurę utworzenia konta maszyny w domenie TEST.

W przypadku sieci o strukturze domeny istnieje możliwość logowania się użytkowników zarówno do lokalnej stacji roboczej, jak i domeny TEST. Wzorce biometryczne mogą być przechowywane:

- lokalnie (ang. *User's local account*) – brak zagrożenia spójności zapisanych wzorców w przypadku „Stacja2", występowanie zagrożenia w przypadku „Stacja1",

- zdalnie (ang. *User's domain account*) – brak zagrożenia spójności zapisanych wzorców dla obu stacji.

W prezentowanym rozwiązaniu istnieją stacje robocze należące do domeny, w której rolę podstawowego kontrolera domeny pełni „Serwer1". Nawiązując do MS Windows NT Server 4.0, zainstalowanego na wspomnianej maszynie, instalacja Biologon Security System v. 2.0, związana jest z dodaniem do systemu następujących podstawowych elementów:

- komponent *Biologon Security* (Panel sterowania),
- opcja „pobierz wzorce biometryczne" (Okno *Windows NT Security*),
- dodatkowe opcje w: *Server Manager*, *User manager for domains*.

Za pomocą aplikacji *Server Manager* możliwe jest ustalanie właściwości systemu biometrycznego danej stacji roboczej (między innymi *Workstation policy*). W przypadku „Stacja2" opcje związane z ustawieniem poziomu bezpieczeństwa są nieaktywne dla wszystkich użytkowników, którzy nie są Administratorami systemu biometrycznego. W przypadku „Stacja1" opcje są aktywne, jednakże z poziomu kontrolera domeny można zmienić aktualne ustawienia poziomu bezpieczństwa. Reasumując, w omawianej konfiguracji występuje możliwość zdalnej administracji systemem.

W celu zapewnienia prawidłowości funkcjonowania Biologon Security System v. 2.0 w strukturze domeny, wykorzystywane są między innymi:

- *BioLogon Authentication Package* (wykonujący weryfikację odcisków palca – spróbkowanego oraz zachowanego, zapewniając w przypadku logowania użytkownika do domeny bezpieczny przesył w czasie zdalnej autentykacji).
- *Biometric Data Storage* (Biologon Security System v. 2.0 przechowuje pobrane wzorce wewnątrz konta użytkownika).
- *Secure Communication Channel* (szyfrowanie procesu komunikacji między stacjami roboczymi a kontrolerami domeny poprzez wymianę klucza publicznego i generowanie losowego klucza sesji).

Na podstawie przedstawionej charakterystyki implementacji w zadanej konfiguracji niniejsze zastosowanie oceniono pozytywnie, zalecając stosowanie.

5. Zalety i wady prezentowanego rozwiązania

Zalety opisywanego rozwiązania:

- prostota obsługi, łatwa i szybka instalacja oprogramowania,
- przyjazny interfejs; możliwość korzystania z kreatorów,
- w określonych aspektach usprawnienie bezpieczeństwa systemu,
- szybka, wygodna autentykacja użytkownika,

- możliwość czytania linii papilarnych pod dowolnym kątem,
- możliwość definiowania więcej niż jednego wzorca dla użytkownika,
- możliwość zdalnej administracji dla środowiska MS Windows NT,
- przechowywanie wzorców biometrycznych w postaci zaszyfrowanej.

Wady opisywanego rozwiązania:

- relatywnie wysoka cena,
- słabe zabezpieczenie przechowywanych wzorców biometrycznych (MS Windows 9x).

6. Podsumowanie i wnioski

W celu zwiększenia bezpieczeństwa występuje konieczność stosowania więcej niż jednej metody zabezpieczeń, nie pozostaje to jednak bez wpływu na funkcjonalność systemu. Istotną grupę metod ochrony stanowią techniki autentykacji użytkowników systemów komputerowych. Dynamicznie rozwijającą się grupą metod są metody biometryczne. W określonych aspektach przewyższają one metody oparte na wiedzy czy materialnych identyfikatorach.

W badaniach wykorzystano konkretne rozwiązanie sprzętowe i programowe. Obok zastosowania indywidualnego analiza implementacji dotyczyła środowisk systemów Microsoft Windows, w których występowały stacje robocze pracujące w strukturze grupy roboczej oraz domeny.

Zastosowanie indywidualne oraz rozwiązanie oparte na strukturze grupy roboczej zostało ocenione negatywnie z uwagi na występowanie ryzyka naruszenia integralności mechanizmu bezpieczeństwa związanego z identyfikacją użytkowników.

Pozytywnie została oceniona implementacja w sieci o strukturze domeny Windows NT. Wyniki przeprowadzonych badań wskazały na dużą zależność poziomu jakości mechanizmów bezpieczeństwa całego systemu od jakości bezpieczeństwa gwarantowanego przez system operacyjny, w którym klient systemu biometrycznego był instalowany.

LITERATURA

1. Praca zbiorowa pod red. Grzywak A.: Bezpieczeństwo systemów komputerowych i telekomunikacyjnych. Wydawnictwo SOTEL, Chorzów 1999.
2. IDENTIX Biologon Security System v. 2.0. User's Guide.

Recenzent: Dr inż. Bartłomiej Zieliński

Wpłynęło do Redakcji 27 lutego 2001 r.

Abstract

In presented paper analysis of utilization of selected method was performed and on that ground appropriate estimation of analyzed method under certain conditions was provided. Presented solution is based on Microsoft Windows operating system environment. Biologon Security System uses special technology along with each user's physical attributes to associate to a user profile and grant access to the system. Installed biometrics system is closely integrated and dependent on operating system installed on given workstation. Two parameters of described system were extremely relevant to quality of entire solution: Workstation policy that determines what methods of logon are available for a user, Logon type that specifies what methods of logon are accepted (per user) by system. Biologon Security System implemented on Microsoft Windows 9x was recognized as a solution that does not fulfill security requirements at demanded level. The main reason of estimating that implementation negatively was lack of mechanism that would let only an Administrator set *User / Workstation policy*. Nevertheless any user of workstation running Microsoft Windows 9x operating system was capable of making damages to the biometrics system through modification of keys in the registry. In a workgroup there is a benefit concerning network installation, but the possibility of making harmful changes that would spoil system integrity still remains. Opposite situation to mentioned above occurs while implementing Biologon Security System v. 2.0. in Windows NT environment. On the assumption that security issue is the most significant matter, choosing that environment is highly recommended and estimated positively. In the latter case biometrics system seamlessly integrates biometrics data with Windows NT Security Architecture. An Administrator can manage (remotely) security configuration of any workstation in the domain. To sum up presented biometrics solution provides more benefits than utilization of classic methods, such as logon using password, but biometrics method is not a perfect, universal method for all cases.