Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze bakalářské práce

Biometrické autentizační metody

Ivana Staňková

Souhrn:

Tato práce se zabývá popisem a výčtem používaných biometrických metod za účelem autentizace uživatele. Z dostupných informací a softwarových nástrojů byly vybrány čtyři biometrické parametry, které byly dále prakticky otestovány na vytvořené databázi o rozsahu 20 osob. Z provedených experimentů dosáhla nejlepších hodnot efektivity identifikace metoda analýzy otisku prstu. Rozpoznání mluvčího, identifikace uživatele dle hlasu, taktéž získala zajímavé výsledky, leč ve srovnání s biometrií otisku prstu dosáhla o přibližně o třetinu menší hodnoty efektivity. Z naměřených výsledků byly rovněž vypočteny intervaly příslušných statistických parametrů pro objektivnější zhodnocení metod. I přes velice dobré výsledky se biometrické metody ukázaly jako příliš časově náročné a ne příliš spolehlivé, aby je bylo možné aplikovat pro praktické využití např. ve společnosti. Z tohoto důvodu je tedy nutné ještě jejich další vývoj, avšak je lze momentálně doporučit jako další úroveň zabezpečení pro jednotlivé uživatele.

Klíčová slova:

biometrie, rozpoznávání, autentizace, identifikace, verifikace, otisk prstu, dynamika stisku kláves, obličej, hlas

Cíl práce a metodika:

Hlavním cílem této práce je zejména vytvořit přehled aktuálně používaných autentizačních metod založených na biometrice včetně používaných technologií snímačů biometrických příznaků, vyhodnocování a chybovost autentizace, a zejména praktické otestování dostupných vhodných softwarových nástrojů. Praktické poznatky budou vyhodnoceny vzhledem k aktuálnímu zabezpečení jedné vybrané společnosti.

Za pomoci dostupných poznatků a sofwarových nástrojů bude vybráno několik biometrických metod, které dále budou testovány z hlediska úspěšnosti autentizace a pohodlnosti pro uživatele při zadávání jeho identity, resp. efektivity snímání. Všechny dostupné nástroje, které budou mít potencionální využití pro praktickou aplikaci ve vybrané společnosti, budou důkladně otestovány na vytvořené databázi tvořenou 20 osobami.

Teoretická část:

Důležitým milníkem pro rozvoj používaných metod zabezpečení byl objev elektrického proudu a jeho následná distribuce. Díky tomuto rozvoji bylo možné zabezpečovací prvky

rozměrově zmenšit, ale také značně zvýšit jejich účinnost, neboť používání digitálních signálů u elektroniky umožňuje použití komplikovanějších otevíracích posloupností atd.

Elektronický zámek má stejnou funkci jako klasický mechanický. Skládá se ze dvou částí- řídící jednotky a klíče, který je nosičem identifikátorů a slouží k odemknutí zámku. Klíč může mít jak fyzickou (přístupová karta), tak i imaginární podobu (např. číselný kód).

Vyhodnocování přístupu je velice důležitou procesní částí zabezpečení. Na základě špatné klasifikace během vyhodnocovací fáze může dojít k neoprávněnému přístupu či chybnému zamítnutí přístupu. V této fázi zabezpečení je využíváno několik různých klasifikátorů pro udělení či zamítnutí přístupu na základě zkoumaných příznaků. V problematice zabezpečení je vyhodnocovací stupeň složen ze dvou dílčích částí, autorizace a autentizace.

K určení pravosti subjektu jsou vybírány nejvíce unikátní příznaky v rámci zkoumané databáze. Ideálně je jejich hodnota korelace rovna nule. Tohoto předpokladu, že pro každého člověka jsou některé příznaky zcela unikátní a neměnné, využívá právě biometrie, kterou lze definovat jako metodu autentizace založenou právě na biologických příznacích (morfologické a fyziologické).

Praktická část:

Tato část bakalářské práce pojednává o skutečných nástrojích pro účely biometrické autentizace, resp. o jejich vhodnosti zařazení do běžné praxe (Zeman, 2011). Jako modelový příklad, na který budou vybrané způsoby dodatečného zabezpečení aplikovány, byla vybrána jedna nejmenovaná firma z ČR, která se zabývá vývojem softwarového vybavení civilních i vojenských letadel. Jelikož se jedná o firmu, která vytváří produkty citlivé na výrobní tajemství, je zcela nezbytné, aby se žádné informace nedostaly do nesprávných rukou.

Z tohoto důvodu je využíváno k ochraně všech údajů a dat velmi účinné trojstupňové zabezpečení (identifikační karta, zabezpečení od firmy McAfee, mechanický zámek počítače).

Praktická část této práce má objasnit, zda-li by bylo vhodné již tak kvalitní zabezpečení vytvořených dat a firemního know-how vylepšit za pomoci autentizačních biometrických metod. Proto budou dostupné autentizační metody založené na biometrii vhodně vybrány a aplikovány na výše uvedenou firmu, která čítá přibližně 120 zaměstnanců.

Výsledky - Pro účely testování software byla zvolena databáze čítající celkově 20 subjektů. Konkrétně 12 žen a 8 mužů ve věkovém rozmezí 26 až 57 let. Byly analyzovány tyto biometrické parametry pomocí dostupného software:

Otisk prstu - HP Credential Manager; **Dynamika úderu** – KeyTrac;
Obličej – BetaFace API, KeyLemon; **Hlas** - KeyLemon

Pro software, u kterého bylo v rámci testování možné získat hodnoty efektivity ε, byly vypočteny intervalové odhady průměru μ a směrodatné odchylky σ za předpokladu normálního rozdělení a 95% intervalu spolehlivosti (viz Tab. 1).

Tab. 1 Intervalové odhady statistických parametrů vybraných efektivit.

Software	ε [%]	
	Intervalový odhad μ	**Intervalový odhad σ**
HP Credential Manager (μ= 99,815 %; σ= 0,4234 %)	$P(99{,}625 < \mu < 100) = 0{,}95$	$P(0{,}343 < \sigma < 0{,}578) = 0{,}95$
KeyLemon – Hlas (μ= 81,3 %; σ= 18,0447 %)	$P(73{,}186 < \mu < 89{,}414) = 0{,}95$	$P(14{,}617 < \sigma < 24{,}672) = 0{,}95$

Závěr:

Touto prací byla za pomoci pěti různých softwarových nástrojů detailně otestována autentizace za pomoci analýzy jednoho ze čtyř vybraných biometrických znaků. Jak je patrné z naměřených výsledků, všechny metody mají největší slabinu v rychlosti zpracování analyzovaného biometrického znaku, v jeho korektním pořízení pro následnou správnou autentizaci a rovněž v efektivitě autentizačního procesu. Vzhledem k původně zamýšlené aplikaci v menší/střední firmě, velikosti potencionální rizika s přístupy uživatelů k počítačům či do kýžených prostor a cenu za koupi potřebných licencí, nelze žádnou z vybraných biometrických autentizačních metod doporučit pro celkové zabezpečení společnosti, ale pouze pro individuální zabezpečení jako další stupeň ochrany před neoprávněným přístupem. Je tedy zcela evidentní, že dosavadní řešení zabezpečení přístupu pomoci velmi silných hesel a přístupových karet je nejen dostačující, ale efektivnější a spolehlivější než jakákoliv výše prezentovaná biometrická autentizační metoda.

Použitá literatura:

JAIN, A. K. - FLYNN, P. - ROSS, A. *Handbook of Biometrics*. New York: Springer-Verlag, 2008. ISBN 978-0-387-71041-2

RAK, R. - MATYÁŠ, V. - ŘÍHA, Z. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: GRADA, 2008. ISBN 978-80-247-2365-5

RUSS, J. C. - WOODS, R. P. The Image Processing Handbook. *Journal of Computer Assisted Tomography*, 1995, vol. 19, no. 6, p. 979-981.

ZEMAN, T. *Aplikace biometrických systémů*. Praha, 2011. Bakalářská práce. Bankovní institut vysoká škola v Praze. Vedoucí práce Mgr. Miroslav Široký, DiS.