České vysoké učení technické v Praze
Fakulta biomedicínského inženýrství
Katedra biomedicínské informatiky

Autentizace uživatelů pomocí dynamiky pohybů myší

User Authentication Through Mouse Dynamics

Bakalářská práce

Autor bakalářské práce: Anežka Čumrdová
Vedoucí bakalářské práce: Ing. Anna Schlenker

Studijní program: Biomedicínská a klinická technika

Studijní obor: Biomedicínská informatika

19. května 2017

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra biomedicínské informatiky

Akademický rok: 2016/2017

Zadání bakalářské práce

Student: **Anežka Čumrdová**

Obor: Biomedicínská informatika

Téma: **Autentizace uživatelů pomocí dynamiky pohybů myší**

Téma anglicky: User Authentication Through Mouse Dynamics

Zásady pro vypracování:

Cílem bakalářské práce je návrh vlastního řešení zabezpečení malé ordinace za použití behaviorálních biometrických charakteristik se zaměřením na dynamiku pohybů myší.

V bakalářské práci se seznamte s metodami identifikace a autentizace pomocí dynamiky pohybu myší nebo jiných polohovacích zařízení (např. touchpad, trackball, atd.). Vytvořte přehledovou studii v oblasti autentizace pomocí dynamiky polohovacích zařízení. Dále se věnujte analýze použitelnosti jednotlivých metod či konkrétních aplikací v oblasti biomedicíny a zdravotnictví. Dle výsledků analýzy začleňte vybrané metody do provozu malé ordinace tak, aby byly pro personál co nejméně obtěžující a jejich použití co nejméně finančně a technicky náročné.

Seznam odborné literatury:

[1] Rak Roman, Matyáš Václav, Říha Zdeněk a kolektiv, Biometrie a identita člověka, ed. 1, ročník 1, kapitola 17, 2008, Grada Publishing a.s.

[2] Ahmed Awad E. Ahmed, Issa Traore, A New Biometric Technology Based on Mouse Dynamics, IEEE Trans. Dependable Secur. Comput., ročník 4, číslo 3, 2007, Červenec, 165-179 s., DOI=http://dx.doi.org/10.1109/TDSC.2007.70207

Zadání platné do: 11.09.2018

Vedoucí: Ing. Anna Schlenker

.....
vedoucí katedry / pracoviště

.....
děkan

V Kladně dne 20.02.2017

Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem „Autentizace uživatelů pomocí dynamiky pohybů myší“ vypracovala samostatně. Veškerou použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně 19.5.2017 ..... Anežka Čumrdová

Poděkování

Ráda bych touto cestou vyjádřila poděkování Ing. Anně Schlenker za její cenné rady a trpělivost při vedení mé bakalářské práce.

Abstrakt

Autentizace uživatelů pomocí dynamiky pohybů myší

Cílem této práce je návrh řešení zabezpečení za použití behaviorálních biometrických charakteristik se zaměřením na dynamiku pohybů myší. K rozpoznávání uživatelů jsou použity metody identifikace a autentizace na základě behaviorální biometrické charakteristiky, dynamiky pohybů myší. Analýze současného stavu se věnuje přehledová studie, která se zabývá stavem prací v oblasti autentizace pomocí pohybů myší. Výsledkem práce je návrh aplikace, která by měla být schopna staticky ověřovat uživatele. Tato aplikace bude začleněna do zdravotnického provozu v rámci zabezpečení virtuální ordinace.

Klíčová slova

Autentizace; Dynamika pohybů myší; Biometrie; Bezpečnost dat;

Abstract

User Authentication Through Mouse Dynamics

The aim of this theses is to design the security solutions using behavioral biometric characteristics focusing on the dynamics of mouse movements. The user recognition methods, used for identification and authentication, are based on the behavioral biometric characteristic called mouse dynamics. A review study deals with analysis of the current state of work in the area of authentication by mouse movements. The result of the thesis is an application design that should be able to statically authenticate users. This application will be integrated into a healthcare facility as a part of virtual consulting room.

Keywords

Authentication; Mouse Dynamics; Biometrics; Data Security;

Obsah

Seznam symbolů a zkratek

FRR	false rejection rate (chybné odmítnutí)
FAR	false acceptance rate (chybné přijetí)
EER	equal error rate
MDS	mouse dynamic signature (podpis pohybu myši)
PIN	personal identification number (osobní identifikační číslo)

Kapitola 1

Úvod

V dnešní době, v době technického rozvoje se o bezpečnosti začíná mluvit víc a víc, velký důraz je kladen na elektronickou bezpečnost dat. V oblasti zdravotnictví a biomedicíny je nanejvýš důležité data pacientů důkladně chránit. Citlivá data pacientů se uchovávají v nemocničních informačních systémech, kde existují možná rizika a hrozby. U lékařů a zdravotnického personálu, již nejde jen o dodržování lékařského tajemství. Musí si také uvědomit, že veškerá data o pacientech jsou zaznamenávána do informačních systémů, které často bývají lékaři brány jen jako podpůrný systém. Proto tyto systémy často nepodléhají dostatečné kontrole.

Biometrické ověřování uživatele se dostává do hledáčku vědců, protože se to zdá jako vhodné řešení elektronické bezpečnosti na rušných zdravotnických pracovištích, kde se vyskytují citlivá data o pacientech. Použitím biometrických charakteristik pro ověření uživatele se jeví jako vhodné zvýšení stupně zabezpečení.

Práce je rozdělena do několika kapitol. První kapitola se zabývá teoretickými základy práce, kde jsou vysvětleny základní pojmy (identifikace, autentizace a autorizace). Dále je popsána samotná biometrie, která se dělí dle charakteristik na behaviorální a anatomicko-fyziologickou. Tyto charakteristiky jsou dále popsány a vysvětleny. Je zde vysvětleno jak se měří výkonnost systémů a popsána problematika chybovosti. Podrobněji je v této kapitole zpracována oblast dynamiky pohybů myší a její výhody a nevýhody.

Přehledová studie shrnuje v jaké době se začala behaviorální biometrie více rozvíjet, na co biometrie dynamiky pohybů myší navazuje a jak se dělí. Jsou zde popsány různé experimenty, které ne vždy dosahují hodnot pro splnění Evropské normy.

V další kapitole popisuji volně dostupnou aplikaci na zachytávání a měření pohybů myší. Dále následuje se návrh vlastního řešení autentizace uživatelů pomocí dynamiky pohybů myší.

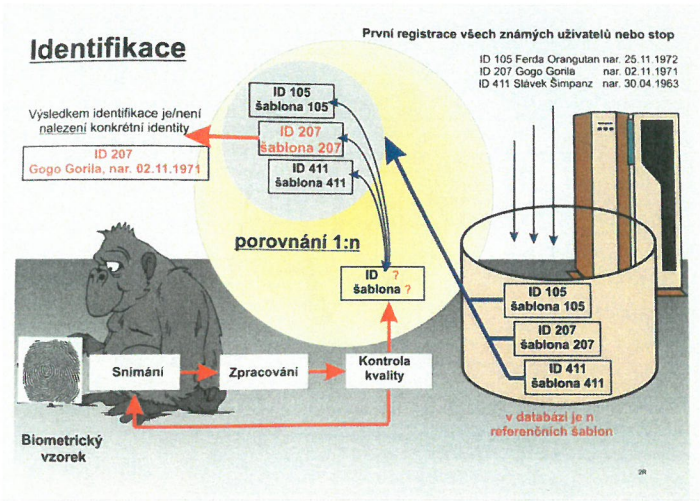
Kapitola 2

Teoretické základy práce

2.1 Identifikace a autentizace

2.1.1 Identifikace

Identifikace je proces porovnávání, ztotožnění kdo je daná osoba. Požaduje se, aby uživatel udal svoji identitu před tím, než bude jeho biometrická informace porovnána. Biometrický údaj, který uživatel poskytne se porovnává se všemi referenčními vzorky v databázi, dokud nedojde k nalezení shody (*"One-To-Many Matching"* – jeden k mnoha, *1:n* [1]).



Obrázek 2.1: Identifikace v počítačové databázi [1].

2.1.2 Autentizace

Autentizace může probíhat po identifikaci. Prověřuje pravost identity tak, že porovnává biometrický vzorek se šablonou referenčního vzorku (*"One-To-One Matching"* – jeden k jedné, *1:1* [1]). Autentizace může být dosaženo třemi způsoby [2].

1. Něčím co uživatel *zná* – tzv. znalostní faktor (např. přístupové heslo, PIN), tato metoda autentizace je velice oblíbená a často používaná. Zároveň v sobě ukrývá nedostatky. Většinou špatně zvolená hesla (krátká, klíčová slova) nebo potřeba pravidelně měnit heslo, které si pak uživatel nepamatuje, jsou největší nedostatky této metody. V krajním případě si uživatel heslo zapíše (na nástěnku, na lísteček nebo do mobilu). Tímto chováním se výrazně zvyšuje riziko zneužití a odcizení hesla.

2. Něčím co uživatel *vlastní* – tzv. vlastnický faktor. Osoba prokazuje svou totožnost něčím co vlastní (identifikační doklady, čipová karta, klíč). U této metody je vysoké riziko odcizení nebo ztracení daného předmětu což může vést k jeho zneužití.

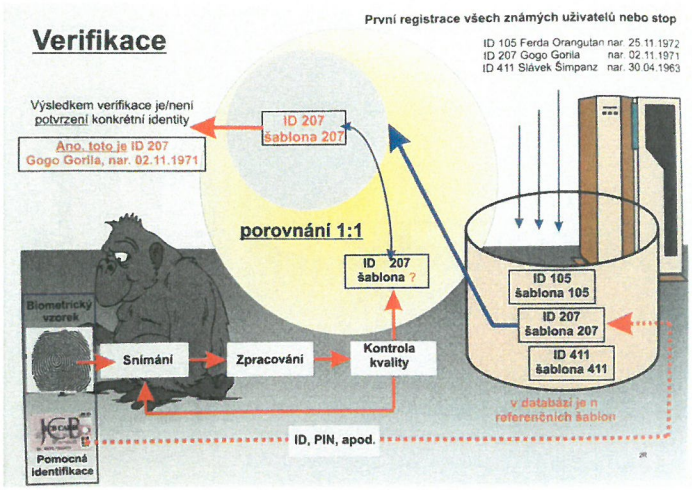
3. Něčím co uživatel *je* – tzv. biometrický faktor (např. otisk prstu, hlas) je jedinečný a unikátní pro každého jedince. Proto tuto metodu lze jednoznačně použít k prokázání identity osoby. Identitu dané osoby je téměř nemožné napodobit nebo odcizit [1].

V současnosti se často využívá tzv. *multi-faktorová autentizace.* Je to z důvodů, že to, co máme nám může být ukradeno nebo napodobeno; to, co známe a umíme, může být odpozorováno, uhodnuto nebo jinak získáno. Obě tyto možnosti mohou být tedy zneužity jinými osobami než je oprávněný uživatel. Proto se v praxi setkáváme s kombinováním znalostního s vlastnickým faktorem autentizace, aby případné riziko zneužití bylo minimální [1].

Nejlepší způsob zabezpečení je použití všech tří faktorů. Kombinace obvyklého hesla a použití čipové karty spojeno s biometrikou jako například geometrie ruky, otisky prstů, rozpoznávání tváře, ověření hlasu, psaní na klávesnici nebo snímání pohybů myší.

2.1.3 Verifikace

Verifikace je proces ověření bez předchozí identifikace, tj. systém sám rozpozná uživatele.



Obrázek 2.2: Verifikace v počítačové databázi [1].

2.1.4 Autorizace

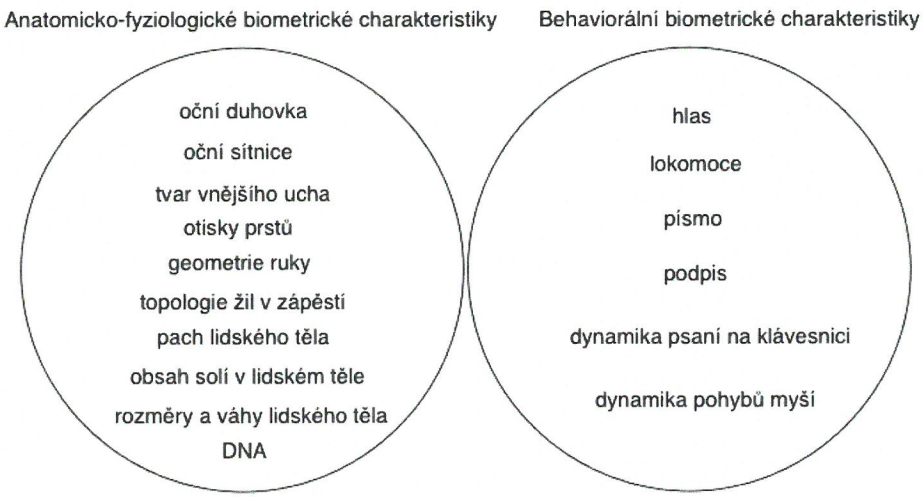
Autorizace ve většině případů navazuje na autentizaci. Je to proces získávání finálního souhlasu, že je uživatel oprávněný a může tedy sytém používat. Podstatou je ověřit, zda má daný uživatel oprávnění provádět příslušnou akci. Autorizace je prováděna operačním systémem nebo k tomu určeným softwarem.

2.2 Biometrie

Existují dva typy biometrických systémů, které propojují osobu s její identitou, verifikace a identifikace [3]. Biometrická verifikace/identifikace je využití jedinečných, měřitel-ných, fyzikálních nebo fyziologických znaků (tzv. markantů) nebo projevů člověka k jednoznačnému zjištění (identifikace) nebo ověření (verifikace) jeho identity [1]. Biometrická identifikace osob je tedy založena na anatomicko-fyziologických nebo behaviorálních charakteristikách každého lidského jedince. Každý biometrický systém by měl splňovat sedm základních podmínek [3].

1. *Univerzálnost* – Každý jedinec by měl mít charakteristiky.

2. *Unikátnost* – Žádné dvě osoby nesmí mít stejné biometrické vlastnosti.
3. *Stálost* – Vlastnosti jedince by neměly být proměnné s časem.
4. *Získatelnost* – Vlastnosti musí být měřitelné kvantitativně a snadno dostupné.
5. *Přesnost* – Úroveň přesnosti biometrické techniky, s kterou lze danou charakteristiku změřit.
6. *Přijatelnost* – Úroveň uživatelského přijetí biometrickým systémem musí být dostačující pro daný systém.
7. *Odolnost* – Míra obtížnosti za účelem falešné identifikace/autentizace.



Obrázek 2.3: Členění biometrické identifikace, inspirované [1].

2.2.1 Anatomicko-fyziologické biometrické charakteristiky

Jsou charakteristiky, které má každý jedinec často vrozené, takže se nedají příliš ovlivnit. Jsou jedinečné a v čase většinou neměnné. Poskytují jednorázovou autentizaci, ale je nutný specializovaný hardware, který není vždy levný nebo přístupný na uživatelských přístrojích [4]. Některé přístroje mohou být pro uživatele i nepříjemné. Nejpoužívanější charakteristiky jsou např. [1], [2]:

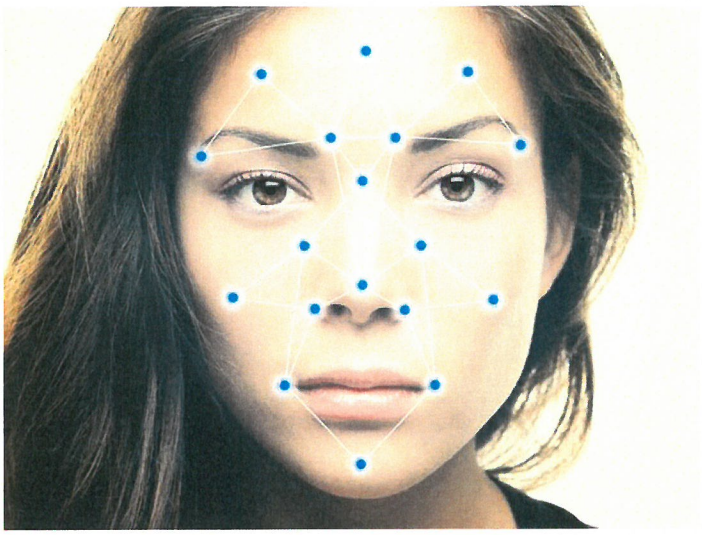
- Otisky prstů – měření unikátních obrazců papilárních linií na prstech (Obrázek 2.4). Otisky prstů jsou celosvětově uznávány jako standard policejně-soudní i bezpečnostně-komerční identifikace. Snímání probíhá pomocí snímacích senzorů, které může rozdělit na senzory kontaktní (např. optické, elektronické, tlakové nebo teplotní) a senzory bezkontaktní (optické a ultrazvukové). Bezkontaktní způsob snímání otisků eliminuje dotyky špinavých prstů, avšak například teplotní kontaktní senzor dokáže rozpoznat, zda daný otisk patří živé osobě a nejedná se tedy o neživý padělek.

Obrázek 2.4: Daktyloskopické vzory [1].

- Geometrie ruky – měří se výška, šířka a délka jednotlivých prstů, kloubů a kostí. Tato metoda je poměrně jednoduchá a rychlá, často se kombinuje se znalostním faktorem například se zadáním PINu (Obrázek 2.5) nebo vložením identifikační karty; tato metoda může být náchylná na třírozměrné padělky dlaně.

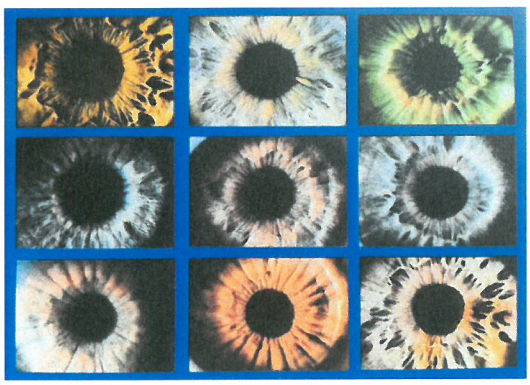
Obrázek 2.5: Zařízení pro snímání tvaru lidské ruky [5].

- Tvář – je vlastní pro každou osobu. Postavení a tvar nosu, postavení lícních kostí, očních důlků a úst, tyto identifikační (antropologické) body jsou specifické a časově neměnné (Obrázek 2.6).



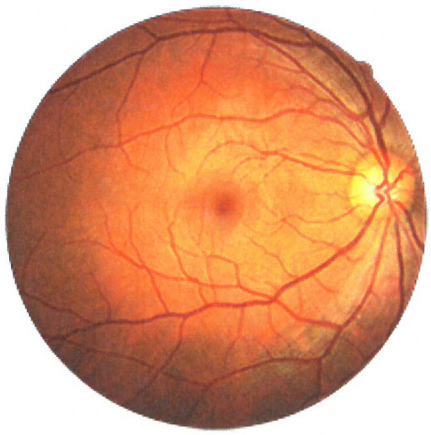
Obrázek 2.6: Identifikační body lidské tváře [6].

- Oční duhovka – je barevný kruh kolem zorničky lidského oka, kde se nachází unikátní identifikační body, podle kterých se s velkou přesností dá určit identita osoby. Žádné dvě duhovky oka nejsou stejné (Obrázek 2.7). Skládají se z barevných struktur, které jsou v čase neměnné.



Obrázek 2.7: Fotografie duhovek lidského oka [1].

- Oční sítnice – pomocí světelných paprsků dopadajících na sítnici se zmapuje řečiště drobných cévek a žilek v zadní části oka, které jsou během života téměř neměnné (Obrázek 2.8).



Obrázek 2.8: Snímek lidské sítnice s vrstvou cév [7].

- DNA – ukrývá v sobě obrovské množství informací o osobě. Již nepatrná část, stačí k určení identity osoby pomocí tzv. genetického otisku jedince (Obrázek 2.9).

Obrázek 2.9: DNA [8].

2.2.2 Behaviorální biometrické charakteristiky

Jedná se o vlastnosti, které jsou založené na chování osob. Tyto atributy se mohou v průběhu života měnit, jsou to vlastnosti, které mohou být naučené i natrénované. Zároveň tyto biometriky nemohou (u většiny případů) být zapomenuty, ukradeny nebo ztraceny. Většina behaviorálních charakteristik je proměnná v čase, takže biometrický systém musí být dynamický a schopný akceptovat určitý stupeň variability. K zachycení biometrických údajů stačí běžně dostupný hardware (např. myš, klávesnice, kamera, mikrofon). Měření je obvykle méně obtěžující a finančně náročné než měření anatomicko-fyziologických charakteristik [9].

Mezi behaviorální biometrické metody patří [1]:

- lidský hlas – zpracovává se tón, intenzita a rytmus hlasu, tyto charakteristiky často nelze zaměnit nebo zapomenout,
- podpis – vyhodnocují se statické i dynamické charakteristiky při jeho psaní, např. rychlost psaní, přítlak, směr podpisu nebo kombinace vzhledu,
- dynamika stisku počítačových kláves – měří se jednotlivé údery na klávesnici, doba stisku klávesy nebo čas uplynulý mezi stisky jednotlivých kláves,
- dynamika pohybu myší – zpracovává se záznam o pohybu myši, vzdálenost, rychlost a další charakteristické vlastnosti.

U všech těchto biometrik se můžeme potýkat s řadou komplikací. Například když je člověk ve stresu nebo naopak rozradostněn, může dojít ke změně chování, které má vliv na snímání těchto charakteristik. To samé platí, když si uživatel například zlomí ruku nebo onemocní. Snímače pak uživatele mohou označit za neoprávněnou osobu.

2.2.3 Měření výkonnosti biometrických metod a zařízení

Chybovost je při těchto metodách vždy přítomna. Je nemožné aby člověk při autentizaci byl 100% jako při registraci. Proto je nutné povolit určitou odchylku mezi srovnávacími vzorky, to se pak může projevit občasnými chybami v rozhodování.

Biometrický systém rozhoduje zda určí aktivního uživatele jako pravého nebo jako podvodníka. Při každém rozhodnutí může dojít k chybě: chybné odmítnutí (chyba 1. typu) a chybné přijetí (chyba 2. typu). Počet falešných odmítnutí/ falešných přijetí je vyjádřen

jako procento pokusů o přístup. Tyto hodnoty se využívají k vyjádření bezpečnosti systému [3].

False Rejection Rate (FRR)(chybné odmítnutí) je koeficient pravděpodobnosti, že systém nesprávně označí aktivního uživatele za podvodníka, i když ve skutečnosti tomu tak není.

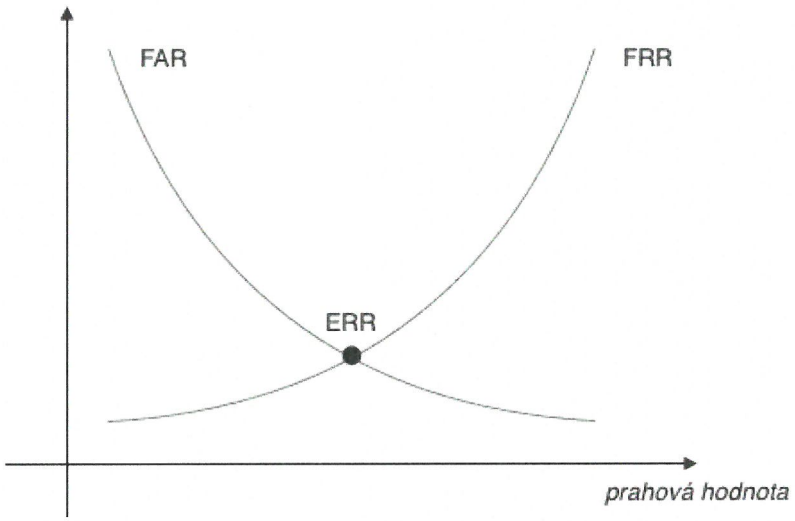
$$\text{FRR} = \frac{\text{počet nesprávných odmítnutí}}{\text{počet všech autentizačních pokusů}} * 100[\%]$$

False Acceptance Rate (FAR)(chybné přijetí) je koeficient pravděpodobnosti, že systém nesprávně označí aktivního uživatele jako stejného uživatele, který dělal zápis podpisu.

$$\text{FRR} = \frac{\text{počet nesprávných přijetí}}{\text{počet všech autentizačních pokusů}} * 100[\%]$$

Verification Time je čas potřebný pro sběr dostatečného počtu dat (údajů) k rozhodnutí o ověření uživatele [9].

Equal Error Rate (EER) je chybovost, když parametry (jako jsou například práh citlivosti) jsou nastaveny tak, že FRR a FAR jsou si rovny. Čím nižší je EER, tím přesnější je systém.



Obrázek 2.10: EER.

Při snímání vzorků je téměř nemožné docílit dvakrát stejného výsledku, v důsledku se pak porovnávané šablony trochu liší. **Míra ztotožnění** (tzv. skóre) je proto pokaždé mírně odlišná. Dále se musí nastavit **práh citlivosti**. Oprávněný uživatel, jenž má skóre vyšší než práh citlivosti, je aplikací akceptován. V opačném případě je odmítnut. Neoprávnění uživatelé, jenž mají skóre vyšší než citlivostní práh, jsou také aplikací přijati. Při hodnotě nižší jsou odmítáni stejně jako oprávnění uživatelé. O oprávněnosti uživatele rozhoduje míra ztotožnění biometrických vzorků.

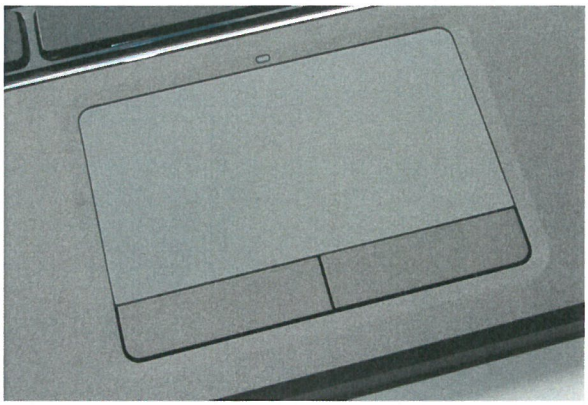
2.3 Dynamika pohybu myší

Tato dynamika popisuje chování jednotlivých polohovacích zařízení, jako je myš, touchpad nebo track ball.

- Myš – klasický přídavný hardware k počítači. Používá se pro ovládání grafického rozhraní používaného operačního systému. Přenáší informace o svém pohybu na pohyb kurzoru po obrazovce. Většinou se na ní nachází dvě tlačítka a kolečko na rolování po obrazovce nahoru a dolu. Snímač pohybu je umístěn zespodu na myši, rozlišuje se na mechanický nebo optický. V dnešní době se můžeme setkat jak s drátovým připojením do počítače, tak s bezdrátovými zařízeními (pomocí infračerveného záření (IrDA) nebo rádiových vln (bluetooth)), která jsou lépe přenositelná.

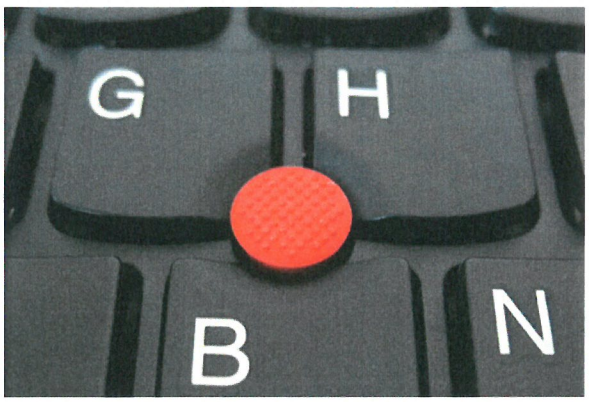
Obrázek 2.11: Počítačová myš [10].

- Touchpad – toto zařízení (destička) se používá zejména u laptopů, ve kterých je vestavěný. Snímá elektrickou kapacitu prstu. Přenáší pohyb prstu po destičce na pohyb kurzoru na obrazovce.



Obrázek 2.12: Touchpad [11].

- Trackpoint – toto polohovací zařízení se většinou vyskytuje v klávesnici laptopů. Dá se ovládat jedním prstem a je to takový malý joystick (pákový ovladač).



Obrázek 2.13: Trackpoint [12].

- Trackball – je kulička, kterou se dá pohybovat pomocí prstů nebo dlaně. Bývá zabudován v počítačové myši nebo je samostatně. Používá se tam, kde je nutná velká přesnost a preciznost.

Obrázek 2.14: Trackball [13].

Dynamika myši je navržena jako behaviorální charakteristika, za předpokladu, že chování myši je relativně jedinečné mezi různými lidmi [9]. Snímání pohybu myší a následný sběr dat je prováděn za použití standardních hardware zařízení, která jsou dostupná u většiny základních počítačů. Z toho vyplývá, že biometrie dynamiky myši může být shromažďována a zpracovávána nenápadně a poté používána k pasivnímu sledování uživatelů počítačů, za účelem detekce útoků.

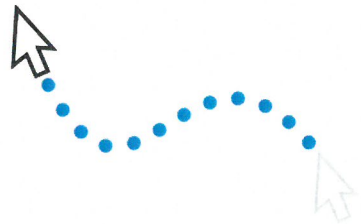
Nevýhodou této metody se může stát vysoká variabilita, která ovlivňuje její přesnost. Lidské chování je totiž charakterizováno nejistotami souvisejícími s řadou faktorů (např. emoční, vliv prostředí, atd.). Silná variabilita údajů lze vysvětlit neschopností člověka reprodukovat stejnou akci s vysokou přesností [14].

Vlastnosti dynamiky pohybů myší lze charakterizovat sadou faktorů generovaných analýzou zaznamenaných akcí myší. Jedná se o faktory reprezentující tzv. „podpis pohybu myší“ (MDS, Mouse Dynamics Signature) konkrétního uživatele, které mohou být použity při ověření totožnosti uživatele. Autentizace pomocí dynamiky pohybů myší může být statická nebo kontinuální. Statická zpracovává a ověřuje data od uživatele v určitém čase (např. při přihlášení), naopak kontinuální verifikace shromažďuje a ověřuje data uživatele opakovaně

po celou dobu trvání relace. Pro identifikaci uživatele musíme shromažďovat údaje o akcích myši, jako např. Mouse-Move, Drag and Drop, Point and Click [15].

Měřitelné akce myši:

- obecný pohyb myši (mouse-move),



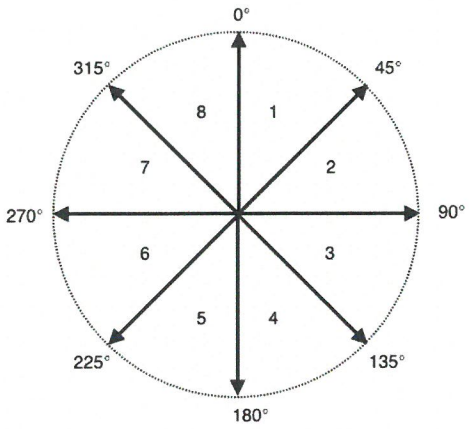
Obrázek 2.15: Pohyb myši [16].

- držení, pohyb a následné uvolnění tlačítka (drag and drop),
- pohyb myši, který je ukončen klikem nebo dvojklikem (point and click),
- doba žádného pohybu myší (silence).

Sledování doby ticha mezi akcemi je důležitý údaj, který může prozradit některé informace o chování uživatele. Rozdílní uživatelé mohou být rozpoznáni jen na základě jejich doby ticha, která může být rozdílná od ostatních. Podle těchto akcí může analýzu dynamiky pohybu myší rozdělit do dvou hlavních kategorií: analýza pohybu a analýza ticha.

Musíme také sledovat jednotlivé charakteristiky [14]:

- typ akce – měřitelné akce myši,
- vzdálenost (v pixelech) – počet pixelů, které kurzor myši „procestuje“ mezi jednotlivými kliky,
- uplynulý čas (v milisekundách) – čas, který je potřeba k vykonání akce,
- směr pohybu – je stanoven na základě úhlu pohybu kurzoru, osm směrů (obr. 2.16), každý z osmi směrů pokrývá soubor pohybů myší prováděných v oblasti 45 °.



Obrázek 2.16: Směry pohybu kurzoru myši, inspirované [17].

Dále záleží na nastavení, které mohou ovlivnit přesnost analýzy biometrických vzorků myši:

- rozlišení obrazovky – jestli byl referenční vzorek snímaný na specifickém rozlišení a analýza prováděna při jiném rozlišení, tak to může mít vliv na rozsah dat a následně na výsledek analýzy,
- rychlosti kurzoru myši – rozdílné rychlosti kurzoru myši mohou mít vliv na získané hodnoty, data nejsou přesná, protože se uživatel musí vypořádat s rozdílným nastavením,
- nastavení tlačítek myši – nastavení tlačítek by měla být stejná na určitém zařízení pro všechny uživatele, aby se daly výsledky vyhodnotit,
- charakteristika hardware – rychlost zařízení, na kterém se autentizace provádí nebo rychlost a typ přídavného hardware, jsou faktory, které mohou zásadně ovlivnit proces sběru dat.

2.3.1 Výhody a nevýhody

Výhody

- Kontinuální ověřování – rozpoznává uživatele během celé relace, aniž by docházelo k narušení činnosti uživatele. Když oprávněný uživatel odejde, nechá počítač přístupný a někdo jiný se mu tam pokusí něco změnit, v takovém případě systém pozná neoprávněného uživatele a odhlásí ho.
- Běžný hardware – ke snímání stačí běžně dostupný hardware jako je myš nebo touchpad, takže finančně nezatěžuje uživatele.
- Absence vlastnického faktoru – není zapotřebí sebou vždy nosit identifikační kartu nebo čip, u kterých je vysoké riziko odcizení nebo ztracení.
- Biometrický faktor – stačí vlastnosti, které nám jsou vlastní. Nemusíme se učit nic navíc nebo si pamatovat složitá hesla.

Nevýhody

- Norma – nebyl vynalezen způsob, který by přijatelně (podle rozsahu normy) rozpoznal správného uživatele jako oprávněného a nesprávného jako podvodníka.
- Změna vlastností v čase – když si jedinec poraní ruku a nemůže s ní vykonávat stejné pohyby, tak aby ho systém rozpoznal jako oprávněného. Stejná situace nastává i když je člověk ve stresu nebo unavený a jeho pohyby myší mohou být odlišné než když je uživatel v naprosté pohodě.
- Nepraktický čas pro ověření – nejdříve se musejí nasbírat a vyhodnotit data, než může začít vlastní verifikace, to trvá u online systémů i několik minut, ve kterých může útočník kompromitovat systém.
- Proměnné prostředí – testovací prostředí se může lišit od prostředí ve kterém bude následná autentizace probíhat.

Kapitola 3

Přehledová studie

Behaviorální biometrie se začala více rozvíjet na začátku 21. století. V tu dobu se značně zvyšovala role biometrik v oblasti bezpečnosti. Od otisků prstů a dalších anatomicko-fyziologických metod se stále více přecházelo na behaviorální metody ověřování, které jsou pro uživatele příjemnější. Nejdříve se řešila dynamika stisku počítačových kláves, jako jedna z behaviorálních charakteristik, která neobtěžuje uživatele a dá se zakomponovat do klasického pracování na počítači.

Později se přidala i dynamika pohybů myší. Nejvíce zmiňovaná je dynamika pohybů myší zaměřovaná na kontinuální verifikaci. Zde je snímáno běžné chování uživatele a při větších odchylkách od normálu může dojít k odhlášení uživatele. Na toto téma bylo zpracováno pár studií, které se různí, od sbírání dat po použité klasifikátory. Výsledky se proto u jednotlivých experimentů značně liší. Je to způsobeno hlavně počtem účastníků studie, dobou trvání nebo jinými měřenými charakteristikami. Další varianta je statická verifikace pomocí dynamiky myši, která nahrazuje klasické přihlašování uživatele pomocí hesla.

3.1 Kontinuální verifikace

3.1.1 Ahmed & Traoré

Studie Ahmed a Traoré [17] se zaměřuje na biometrickou identifikaci, shromažďuje behaviorální vlastnosti uživatele a používá je k zabezpečení počítače. Biometrie dynamiky myši se v tomto případě zaměřuje na tzv. podpis myši, který je založen na vybraných charakteristikách, které jsou vypočítávány pomocí statistických metod, jako jsou například neuronové sítě. Autoři studie vytvořili jeden hlavní experiment a dva menší experimenty.

Hlavní experiment zkoumá, do jaké míry se dá dynamika pohybů myší využít pro pasivní sledování a identifikaci v počítačových systémech. Pro reprodukci skutečných podmínek, umožnili autoři studie účastníkům individuální volbu vybrat si provozní podmínky a aplikace, které budou používat. V důsledku byly shromážděny údaje z různých hardware a software systémů bez omezení na úkony, které uživatelé prováděli.

Druhý a třetí experiment se zabývá vlivem výpočetního prostředí na výsledky prvního experimentu. Zejména operačního systému a použitých aplikací. V obou těchto pokusech jsou operační systém a aplikace pevně nastaveny. Ve třetím experimentu jsou účastníci vyzváni k provádění přesně stejných akcí pomocí speciálně navržené aplikace.

Do hlavního experimentu bylo zahrnuto 22 účastníků, dva malé experimenty zahrnovaly sedm účastníků. Malé experimenty zkoumaly účinky tzv. „zmatených“ faktorů souvisejících s hlavním experimentem.

1. Hlavní experiment: Dvacet dva účastníků bylo požádáno aby si nainstalovali klientský software na svůj osobní počítač. Data, která byla sbírána byla rovnou posílána do centrálního serveru. Úkony, které účastníci prováděli se lišili. Od procházení webu až po hraní her a zpracovávání textů. Celý experiment trval devět týdnů, za tu dobu se stihlo nashromáždit 284 hodin surových údajů o pohybech myší. Bylo nashromážděno kolem 1 000 relací, přičemž průměrně na jednoho člověka připadlo 45 relací. Srovnávání dat od uživatelů probíhá pomocí neuronových sítí, které detekují rozdíly mezi uživateli. Pro každého účastníka se neuronová síť vyškolila během procesu zápisu a pro každého jedince byla připravena jiná kombinace tréninkových dat. Návrh sítě zůstával pořád stejný. Poté bylo použitím one-hold-out křížové validace vypočítáno FAR a FRR. Práh citlivosti byl nastaven na 50 %, z toho vyplývá, že FAR vyšla 2,4640 % a FRR 2,4614 %.

2. Druhý experiment: Účastníci měli za úkol vykonat tři relace, každou s délkou 30 minut. V těchto relacích měli prohlížet Web s aplikace Internet Explorer. Všichni používali stejný hardware a software. Při stejném analyzování dat jako v hlavním experimentu dospěli k výsledku FAR 1,25 % a FRR 6,25 %.

3. Třetí experiment: V tomto posledním testu měli všichni účastníci provést stejný set akcí za použití stejného počítače. Data byla sbírána z devíti relací pro každého uživatele. Výsledná FAR byla 2,245 % a FRR 0,898 %.

3.1.2 Pusara & Brodley

V této studii Pusara a Brodley [18] bylo zkoumáno jestli pohyby myší poskytují přesný model pro identifikaci uživatele, který pohyby provádí. Data byla shromažďována od osmnácti účastníků, kteří pracovali s aplikací Internet Explorer. Nejdříve byl vytvořen model pro normální chování uživatele. Toto vytvoření vyžaduje fázi výcviku, při které jsou shromažďovány údaje o myši uživatele, jsou vybrány modelové parametry a následně vytvořen konečný model. Tento model je pak používán k neustálému sledování účtu pravého uživatele. Pokud se chování uživatele odchýlí od normálního chování je vyzván k opětovné autentizaci nebo vyzván k ohlášení se správci systému.

Pro vytvoření modelu je zapotřebí zachytávat pohyby myší i události myši. Údaje jsou sbírány od osmnácti dobrovolníků. Dostali instrukce používat Windows zařízení a na něm Internet Explorer. Zaznamenány jsou dvourozměrné souřadnice kurzoru v každém detekovaném čase kdy se myš pohnula. Pro extrakci vlastností z dat o pohybech myší je nejprve nutno vypočítat vzdálenost, úhel a rychlost mezi dvojicemi bodů. Po získání potřebných dat dostaneme jejich průměrnou směrodatnou odchylku. Zde se aplikuje řízený algoritmus učení, aby se dalo zjistit, je-li možné určité uživatele od sebe rozeznat na základě pohybů myší. Jako klasifikátor byl v tomto případě použit rozhodovací strom s pomocí smoothing filtru. Výsledné hodnoty FAR a FRR dosahovaly 1,75 % a 0,43 % s verifikačním časem od jedné do patnácti minut.

3.1.3 Gamboa & Fred

V této studii Gamboa a Fred [3] byl vyvinut systém, který zachycuje interakci uživatele pomocí ukazovacího zařízení (myš, touchpad,...), používá informace o chování, k ověření totožnosti jedince. Pomocí statistických metod rozpoznávání byl vyvinut sekvenční klasifikátor, který zpracovává interakce uživatele. Když byla splněna definovaná úroveň přesnosti, identita uživatele se považovala za autentickou, pokud ne, byl uživatel klasifikován jako podvodník.

Byl vyvinut prototyp systému přístupný pomocí webového prohlížeče. Tento systém představuje paměťovou hru pro uživatele. Účastníkova interakce přes webovou stránku je nahrávána a použita k autentizačnímu procesu. Systém je rozdělen na dvě hlavní části:

1. *Systém získávání*, který shromažďuje data a tahy od uživatele a ukládá je do datových souborů.
2. *Systém rozpoznávání*, který čte data ze souborů, klasifikuje údaje o interakcích účastníků. Přičemž odhaduje pravděpodobnost, že aktuální uživatel je skutečným autorem interakce.

Na experimentu se podílelo padesát účastníků, od kterých byla sbírána data. Každý tah byl charakterizován 63 dimenzionálním vektorem zahrnujícím prostorové a časové parametry, jako je úhel a zakřivení, rychlost a zrychlení. Pomocí klasifikátoru byla vypočítána EER pro různý počet tahů. Pro jeden tah, je EER 48,9 %, avšak se vzrůstajícím počtem tahů se EER zmenšuje, již u 50 tahů je EER 2 %, následně u 200 tahů je 0,2 %.

3.1.4 Nakkabi, Traoré & Ahmed

Ve studii Nakkabi, Traoré a Ahmed [14] navrhovaný systém dosahuje velkého zlepšení výkonnosti tím, že vyvíjí samostatné modely pro jednotlivé skupiny vlastností. Vylepšení je dosaženo použitím fuzzy klasifikace založené na učebním algoritmu pro multivariační analýzu dat a použitím score-level fusion (fůze na úrovni skóre) pro sloučení odpovídajících biometrických skóre.

Tento experiment absolvovalo 48 účastníků a hodnocení dosahuje chybného přijetí 0 % a chybného odmítnutí 0,36 %. Tyto výsledky jsou vázané na délku relace. Čím kratší je relace tím lépe, v důsledku to ale znamená méně dat.

Tabulka 3.1: Kontinuální systémy

Zdroj	Rok	FAR	FRR	Počet účastníků	Klasifikátor
Ahmed a Traoré [17]	2007	2,4649 %	2,4614 %	22	Neuronová síť
Pusara a Brodley [18]	2004	1,75 %	0,43 %	18	Rozhodovací strom
Gamboa a Fred [3]	2004	2 %	2 %	50	Sekvenční
Nakkabi, Traoré a Ahmed[14]	2009	0 %	0,36 %	50	Fuzzy logika

3.2 Statická verifikace

Bours a Fullu [19] navrhli přihlašovací metodu pro přístup do systému, za použití dynamiky pohybů myší. Uživatel musí projít s kurzorem myši připraveným bludištěm, mezitím jsou jeho kroky zaznamenávány a používány pro výpočet vektorů rychlosti pro každý úsek cesty. Vzdálenost je používána k porovnání ověřovacích údajů s údaji zápisu. Tohoto experimentu se účastnilo 28 osob. Používali své vlastní počítače a musely použít myš, jiné ukazovací zařízení bylo vyloučeno. V tomto experimentu se uvádí EER 27,5 %.

3.3 Nedostatky prací

Z těchto prací jen jedna splňuje Evropský standard pro poplachové a elektronické systémy, který nastavuje FAR od 1 % do 0,1 %, podle toho jaké hrozí bezpečností riziko. Bezpečnostní riziko je stanoveno na základě hodnoty majetku, který je chráněn a znalostech a způsobu útoku pachatelů.

Při použití biometrie nesmí FAR překročit limit stanovený pro každý stupeň.

- Stupeň 1: nízké riziko. Předpokládá se, že pachatel má malé znalosti systému kontroly vstupu a je limitován omezeným rozsahem snadno dostupných nástrojů. Cílem fyzické

bezpečnosti je odradit a zdržet pachatele. Majetek má limitovanou hodnotu a pachatelé se pravděpodobně vzdají myšlenky na napadení, setkají-li se s minimálním odporem.

- Stupeň 2: nízké až střední riziko. Předpokládá se, že pachatel má malé znalosti systému kontroly vstupu a používá běžný rozsah nástrojů a přenosných přístrojů. Cílem fyzické bezpečnosti je odradit, zdržet a odhalit pachatele. Majetek má vyšší hodnotu a pachatelé se pravděpodobně vzdají myšlenky na pokračování, uvědomí-li si, že mohou být odhaleni.

- Stupeň 3: střední až vysoké riziko. Předpokládá se, že pachatel je obeznámený se systému kontroly vstupu a má ucelený rozsah nástrojů a přenosných elektronických přístrojů. Cílem fyzické bezpečnosti je odradit, zdržet, odhalit a pomoci identifikovat pachatele. Majetek má vysokou hodnotu a pachatelé se pravděpodobně vzdají myšlenky na pokračování, uvědomí-li si, že mohou být chyceni.

- Stupeň 4: vysoké riziko. Předpokládá se, že pachatel má schopnost a prostředky detailně naplánovat napadení a má úplný rozsah přístrojů, včetně prostředků pro nahrazení komponent systému kontroly vstupu. Cílem fyzické bezpečnosti je odradit, zdržet, odhalit a pomoci identifikovat pachatele. Majetek má vysokou hodnotu a pachatelé se pravděpodobně vzdají myšlenky na pokračování, uvědomí-li si, že mohou být identifikováni a chyceni.

Tabulka 3.2: Norma ČNS EN 60839-11-1

	stupeň 1	**stupeň 2**	**stupeň 3**	**stupeň 4**
FAR	1 %	0,3 %	0,3 %	0,1 %
příklad zařízení	hotel	obchodní kanceláře, malé firmy	průmysl, finanční instituce	vysoce citlivé prostory (vojenské zařízení, vládní budovy,..)

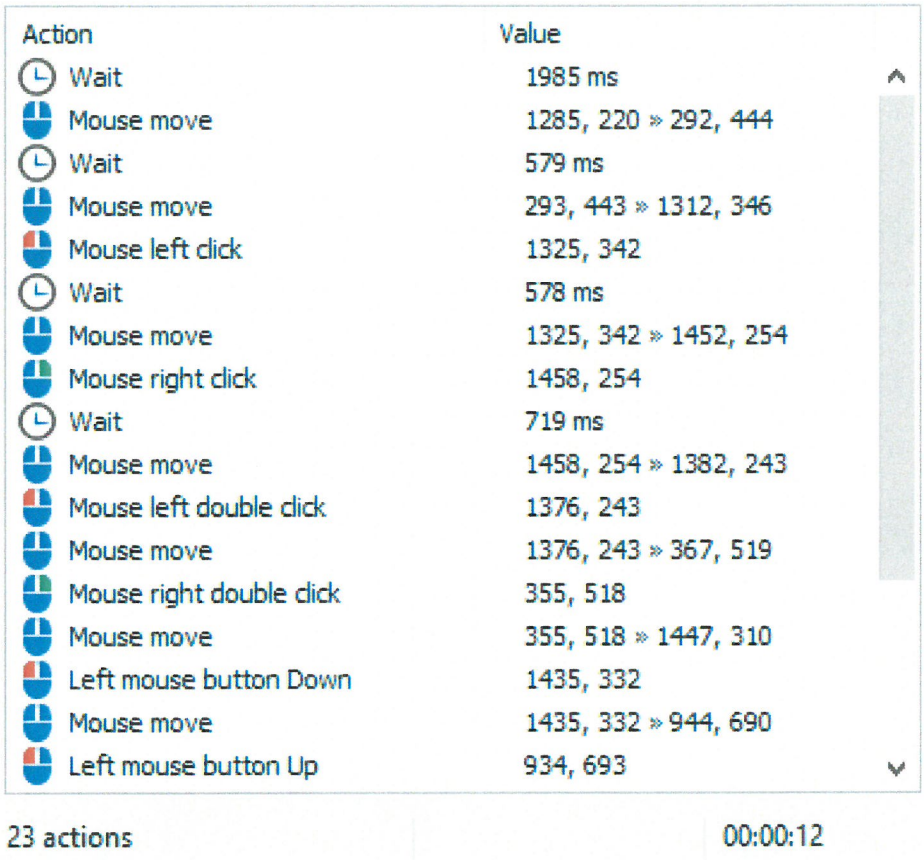
Kapitola 4

Analýza použitelnosti

4.1 MouseRecorder

Testovala jsem aplikaci MouseRecorder, která je dostupná a volně šiřitelná pro počítače s operačním systémem Windows. Tato aplikace zaznamenává pohyb myši, aby ho následně mohla zopakovat.

Aplikace zaznamenává všechny měřitelné akce myši, které jsem popsala již dříve. Čas kdy myš nic nedělá tzv. silence měří v milisekundách, u ostatních akcí vždy ukazuje jen počáteční a koncové souřadnice obrazovky v pixelech. Bohužel se v hlavním okně neukazuje čas, který byl potřeba k vykonání akce. Je viditelný pouze celkový čas relace. Dále je zde hodnota, která nám říká kolik jsme udělali akcí celkem. Čas, který jsme vynaložili na jednotlivé akce myši je možno najít po delším hledání v detailu samostatných akcí. Dále zde není možno vidět směr pohybu kurzoru, jen souřadnice odkud kam se myš pohybovala. Z toho se dá samozřejmě směr vypočítat, ale v ideálním případě by to měla aplikace umět zobrazit. Celý nahrávaný záznam je možno uložit a spustit znovu.



Obrázek 4.1: Aplikace MouseRecorder s naměřenými daty.

4.2 Návrh vlastního řešení

V prostředí zdravotnických zařízení je vhodnější použití statické verifikace na začátku relace, která ověřuje uživatele místo klasického zadávání hesla. Je přesně dané okno, ve kterém se kurzor myši pohybuje. Toto okno je pro všechny typy monitorů stejně velké, má statický počet pixelů, aby se eliminovala rozdílnost prostředí. Uživatel musí splnit sérii úkonů, které by jedince otestovaly jestli je právě on oprávněný uživatel nebo podvodník.

Ve statickém okně se nacházejí čtverečky a náhodně se v nich ukazují čísla od jedné do deseti. Uživatel musí postupně naklikat všech deset čísel správně. Všichni uživatelé mají na tyto úkony pevně stanovený časový limit. Poté se data nahrávají a automaticky posílají na autentizační server, který umožní přístup na základě správnosti dat konkrétního uživatele. Měří se časová odezva jednotlivých kliků, úhel směru myši, rychlost, pohyby myší i například doba ticha mezi jednotlivými kliky.

Z těchto dat se získal průměr, směrodatná odchylka a další faktory, které ovlivňují autentizaci a tyto informace se porovnají s předem daným prahem citlivosti. Na základě výsledků se určí, jestli je uživatel oprávněn pro vstup do systému nebo ne.

Další možnost použití dynamiky pohybů myší vidím ve spolupráci s dynamikou psaní na klávesnici. Tyto dvě charakteristiky společně by mohli docílit sběru více dat, což by vedlo k přesnějším výsledkům. Kontinuálně by se snímali pohyby myši a stlačování kláves na klávesnici. Takže kdyby se u počítače měnili lidé, a používali by jenom myš nebo jenom klávesnici, tak by bylo pořád možné odhalit podvodníka.

Kapitola 5

Diskuze

Dle údajů v této práci můžeme vidět, že behaviorální biometrika pomocí dynamiky pohybů myší zatím nemá obstojné zastoupení na trhu s bezpečnostními aplikacemi. Proto tato metoda pro lékaře a ostatní zdravotnický personál v dnešní době nemá v ordinacích své místo.

Kdyby se přece jen našel způsob jak splnit Evropskou normu, tak by to bylo přínosné nejen pro malé ordinace, ale i pro velké nemocnice, kde se u jednoho zařízení může vystřídat více lidí. Systém by pak byl schopen rozpoznat jaký zaměstnanec dělal jaké operace s myší. Tato metoda by byla efektivnější kdyby se zkombinovala s dynamikou psaní na klávesnici, aby se dosáhlo větší přesnosti systému.

Kapitola 6

Závěr

Výsledkem této práce je seznámení se z problematikou autentizace uživatelů pomocí biometrie a konkrétně dynamiky pohybů myší. Tato metoda by mohla být z výhodou použita v oblasti zdravotnictví a biomedicíny pro svoji jednoduchost na obsluhu, díky absenci kupování dalších drahých přístrojů (postačí klasický hardware) je tato metoda pro nemocnice finančně nenáročná. Z toho vyplývá, že není potřeba složité zaškolování personálu. Takto se může nenásilně zvýšit zabezpečení dat pacientů, které jsou sbírány a ukládány ve zdravotnických informačních systémech.

Tato práce podává rozsáhlejší znalosti o autentizaci a identifikaci uživatele a objasňuje fungování těchto metod spojených s dynamikou pohybů myší. Rešeršní část objasňuje jak fungují jednotlivé experimenty a jejich problematiku.

Řešení nabízí návrh aplikace, která využívá statickou identifikaci uživatele za pomocí dynamiky pohybů myší. Tato metoda se dá nejlépe použít na přihlašování uživatele do systému, čímž snižuje pravděpodobnost bezpečnostního rizika.

Seznam použité literatury

[1] R. Rak, V.Matyáš, and Z. Říha. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích.* Grada Publishing a.s., 2008.

[2] A. Schlenker and M. Šárek. Behaviorální biometrie pro multifaktorovou autentizaci v biomedicíne. *European Journal for Biomedical Informatics*, 8(5):cs18–cs23, 2012.

[3] H. Gamboa and A. Fred. A behavioral biometris system based on human computer interaction. Technical report, Escola Superior de Tecnologia de Setúbal, 2004.

[4] A. Paloski N. Zheg and H. Wang. An efficient user verification system via mouse movements. Technical report, Department of Computer Science, October 2011.

[5] `https://www.tensor.co.uk/time-and-attendance/hand-scanner-terminal/`.

[6] `https://au.pinterest.com/pin/135600638760288639/`.

[7] `http://www.reeveseyeinstitute.com/eye-care-services-johnson-city.htm`.

[8] `https://www.tes.com/lessons/WE5E9RncBhieAQ/dna`.

[9] Z. Jorgensen and T. Yu. One mouse dynamis as a behavioral biometrric for authentication. Technical report, ASIACCS '11, 2011.

[10] `hhttps://mysi.heureka.cz`.

[11] `https://en.wikipedia.org/wiki/Touchpad`.

[12] `https://www.aliexpress.com/cheap/cheap-trackpoint.html`.

[13] `http://www.logitech.com/en-us/product/wireless-trackball-m570`.

[14] I. Traoré Y. Nakkabi and A. A. E. Ahmed. Improving mouse dynamics biometric performance using variance reduction via extractors with separate featured. Technical report, IEEE, November 2010.

[15] S. Benson E. Raj and A. Thomson santhosh. A behavioral biometrics approach based on satndardized resolution in mouse dynamics. Technical Report 4, IJCSNS, 2009.

[16] `http://www.mouserecorder.com/docs/09/manual.htm`.

[17] A. Awad E. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. Technical Report 3, IEEE Transactions on Dependable and Secure Computing, September 2007.

[18] M. Pusara and C.E. Brodley. User re-authentication via mouse movements. Technical report, VizSEC/DMSEC'04, 2004.

[19] P. Bours and CH. J. Fullu. A login system using mouse dynamics. Technical report, IEEE, 2009.

Seznam obrázků

Seznam tabulek

Seznam příloh

Přílohy na CD

Příloha 1 Abstrakt česky (abstrakt.pdf)

Příloha 2 Abstrakt anglicky (abstract.pdf)

Příloha 3 Naskenované zadání BP (zadani.jpeg)

Příloha 4 Kompletní bakalářská práce (BPCumrdova.pdf)