Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra Informačních Technologií

Bakalářská práce

Zabezpečení autentizace do internetového bankovnictví s využitím biometrie

Zdeněk Olič

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zdeněk Olič

Systémové inženýrství a informatika
Informatika

Název práce

Zabezpečení autentizace do internetového bankovnictví s využitím biometrie

Název anglicky

Securing authentication to internet banking using biometrics

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku zabezpečení autorizace internetového bankovnictví.

Hlavní cíl bakalářské práce je zhodnotit metody biometrického zabezpečení vhodné pro posílení zabezpečení autentizace klienta do internetového bankovnictví.

Dílčí cíle práce jsou:
- charakterizovat zabezpečení autentizace uživatele do internetového bankovnictví a biometrickou ochranu,
- analyzovat autentizaci internetového bankovnictví vybraných bank,
- analyzovat vybrané dostupné biometrické metody,
- navrhnout nasazení vybrané biometrické metody do internetového bankovnictví pro zajištění bezpečnosti autentizace uživatele.

Metodika

Teoretická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů, dále bude analyzována autorizace do internetového bankovnictví u pěti největších bank (dle počtu klientů) v České republice. Praktická část práce bude vycházet z analýzy biometrických metod. Budou zhodnoceny jednotlivé vybrané biometrické metody dle kritérií pro biometrické technologie a dále bude měřena jejich výkonnost podle kritérií FAR (False Acceptance Rate) a FRR (False Rejection Rate). Na základě zjištěných poznatků bude navrhnuta koncepce zabezpečení autentizace s využitím biometrické metody. Syntézou teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

biometrie, internetové bankovnictví, otisk prstu, verifikace obličejem, verifikace hlasem, autentizace, verifikace

---

Doporučené zdroje informací

BITTO, O. Šifrování a biometrika aneb tajemné bity a dotyky. Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5

Kala Jan. Internetové Bankovnictví. Praha : Computer Press, 2000.ISBN 80-7226-328-5.

MÁČE, M. *Platební styk : klasický a elektronický.* Praha: Grada, 2006. ISBN 80-247-1725-5.

Marcin Kotarba. "Strategies for Developing On-Line Business Models in Retail Banking". Studia i Materiały 1/2:90-104, Poland 1/2/2018

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

Rathod, V.J. , Iyer, N.C. , Meena, S.M. A survey on fingerprint biometric recognition system. 1st International Conference on Green Computing and Internet of Things, ICGCIoT 2015. ISBN: 978-146737909-0

Vašek Matyáš. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno : Masarykova univerzita, 2008. ISBN 978-80-210-4556-9

Vejnar Jiří. Homebanking.Praha: PC WORLD, 2001.

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Michal Stočes, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 29. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 31. 01. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zabezpečení autentizace do internetového bankovnictví s využitím biometrie" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 10.2.2021 _____

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu práce panu Ing. Michalovi Stočesovi, Ph.D. za jeho mentoring a vedení při psaní bakalářské práce. Dále bych poděkoval své rodině za trpělivost při mém studiu.

Zabezpečení autentizace do internetového bankovnictví s využitím biometrie

Abstrakt

Bakalářská práce se zabývá problematikou zabezpečení internetového bankovnictví. Zabezpečení internetového bankovnictví bude realizován přidáním biometrické metody jako další fáze autentizace klienta do Internetového bankovnictví. Práce se věnuje biometrii a hodnocení biometrických metod, z kterých se vybere jedna podle kritériích pro biometrická zařízení, výkonosti a poslouží k návrhu tří fázové autentizace klienta do Internetového bankovnictví. Řešená část Bakalářské práce se věnuje Internetovému bankovnictví, možnosti autentizace klienta do Internetového bankovnictví a výčtem možností autentizace klienta do internetového bankovnictví u vybraných bank.

Klíčová slova: biometrie, internetové bankovnictví, otisk prstu, verifikace obličeje, verifikace hlasem, autentizace, verifikace.

Securing authentication to internet banking using biometrics

Abstract

The bachelor's thesis deals with the issue of Internet banking security. Internet banking security will be implemented by adding the biometric method as the next phase of client authentication to Internet banking. The work is devoted to biometrics
and evaluation of biometric methods, from which one will be selected according to the criteria for biometric devices, performance and will be used to design three-phase authentication of the client to Internet banking. The solved part of the Bachelor's thesis deals with Internet banking, the possibilities of client authentication to Internet banking, and the list of possibilities of client authentication to Internet banking at selected banks.

Keywords: biometrics, internet banking, finger print, face verification, voice verification, authentication, verification.

Obsah

1 Úvod 12

2 Cíl práce a metodika 13

3 Teoretická východiska 14

3.1 Internetové bankovnictví 14

3.2 Využití biometrie pro zabezpečení 24

3.3 Měření výkonosti biometrických metod a zařízení 35

4 Vlastní práce 38

4.1 Verifikace otiskem prstu 38

4.2 Verifikace tváří 41

4.3 Verifikace hlasem 43

4.4 Vyhodnocení biometrických metod otisk prstu, tvář a hlas 46

4.5 Návrh koncepce zabezpečení autentizace s využitím biometrické metody 48

5 Výsledky a diskuse 59

5.1 Verifikace biometrickou metodou Otisk prstu 59

5.2 Verifikace biometrickou metodou Tvář 60

5.3 Verifikace biometrickou metodou Hlas 60

5.4 Model třífázové autentizace s využitím biometrické metody otisk prstu 61

6 Závěr 62

7 Seznam použitých zdrojů 63

8 Přílohy 68

Seznam obrázků

Obrázek 1 Tři základní vzory papilárních liniích 27
Obrázek 2 Vyznačené markanty na otisku prstu 28
Obrázek 3 Základní druhy markantů 28
Obrázek 4 Optický snímač otisku prstu 29
Obrázek 5 První fáze autentizace 50
Obrázek 6 Druhá fáze autentizace 55
Obrázek 7 Třetí fáze autentizace 58

Seznam rovnic

Rovnice 1 Pravděpodobnost chybného odmítnutí 36
Rovnice 2 Pravděpodobnost chybného odmítnutí jako poměr dvou ploch 36
Rovnice 3 Pravděpodobnost chybného přijetí 37
Rovnice 4 Pravděpodobnost chybného přijetí jakopoměr dvou ploch 37
Rovnice 5 Variace s opakováním 51
Rovnice 6 Variace s opakováním 56

Seznam tabulek

Tabulka 1 Metody autentizace klienta do internetového bankovnictví u České spořitelny 20
Tabulka 2 Metody autentizace klienta do internetového bankovnictví u ČSOB 21
Tabulka 3 Metody autentizace klienta do internetového bankovnictví u Komerční banky 22
Tabulka 4 Metody autentizace klienta do internetového bankovnictví u Monety 23
Tabulka 5 Metody autentizace klienta do internetového bankovnictví u Fio banky 24
Tabulka 6 Operační kritéria zhodnocení 46
Tabulka 7 Finanční kritéria zhodnocení 48
Tabulka 8 FRR a FAR kritéria zhodnocení 48

Seznam použitých zkratek

PSD2 (Payment Service Directive) – Směrnice o platebních službách

SCA (Strong Customer Authentication) – Silné ověření zákazníka

SMS (Short Message Service) – krátká textová zpráva

FAR (False Acceptance Rate) – pravděpodobnost chybného přijetí

FRR (False Rejection Rate) – pravděpodobnost chybného odmítnutí

PUK (Personal Unlocking Key) – osobní odblokovací kód

PIN (Personal Identification Number) – osobní identifikační číslo

PA (Passwords Attack) – heslový útok

PCA (Password Cache Attack) – útok do mezipaměti hesel

PBFA (Preliminary Brute Force Attack) – předběžný útok hrubou silou

FPA (Found Passwords Attack) – hledání hesla útok

CCD (Charge Coupled Device) – zařízení s vázanými náboji

SPL (Sound Pressure Leve) – hladina akustického tlaku

MPx (Mega pixel) – milion pixelů

1 Úvod

Internetové Bankovnictví je jedno z nejvíce používaný a využívaný metody bankovnictví, které v dnešní době nabízí a vede každá banka na světě a je součástí každého vedeného účtu klienta. Mnoho bank využívá internetové bankovnictví jako, prostředek bezkontaktního vedení účtu a komunikace mezi klientem a bankou, nazývaný „Online banking. V české republiky využívá internetové bankovnictví 5,5 milionu lidí (Cieslar, 2019) a počet stále roste a růst bude, kvůli možnostem a výhodám, které nabízí jak Bance, tak klientovy banky.

Rozvoj a možnosti co nabízí dnešní internetové bankovnictví má, ale i své bezpečností problémy. Každá banka používá pro svoje internetové bankovnictví dvou až tří fázovou autentizaci, která slouží k ověření klienta při přihlášení a dále při ověřování poslání platby a dalších možností co nabízejí jednotlivé internetové bankovnictví každé banky. Toto zabezpečení, ale nebere v úvahu bezpečností riziko „lidský faktor“. Jeden z vážných problémů, každého zabezpečení, který lze dobře a jednoduše zneužít. Bakalářské práce se zabývá návrhem nové bezpečnostní tří fázové autentizace, která bude využívat v dnešní době už dostupnou technologii pracující s biometrii lidského těla a umožnila by bezpečnou autentizaci klienta do internetové bankovnictví, která by umožnovala ukončení autorizace požadavků klienta v internetovém bankovnictví, zjednodušila práci klientovy v internetovém bankovnictví, umožnila založení a vyřízení hypotéčních úvěrů, půjček a kontokorentu v internetovém bankovnictví a snížila náklady na pobočky Bank.

2 Cíl práce a metodika

Cíl práce:

Bakalářská práce je tematicky zaměřena na problematiku zabezpečení autorizace internetového bankovnictví.

Hlavní cíl bakalářské práce je zhodnotit metody biometrického zabezpečení vhodné pro posílení zabezpečení autentizace klienta do internetového bankovnictví.

Dílčí cíle práce jsou:

- charakterizovat zabezpečení autentizace uživatele do internetového bankovnictví a biometrickou ochranu,
- analyzovat autentizaci internetového bankovnictví vybraných bank,
- analyzovat vybrané dostupné biometrické metody,
- navrhnout nasazení vybrané biometrické metody do internetového bankovnictví pro zajištění bezpečnosti autentizace uživatele.

Metodika:

Teoretická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů, dále bude analyzována autorizace do internetového bankovnictví u pěti největších bank (dle počtu klientů) v České republice. Praktická část práce bude vycházet z analýzy biometrických metod otisk prstu, tvář a hlas z teoretické části práce. Budou zhodnoceny jednotlivé vybrané biometrické metody dle kritérií pro biometrické technologie a dále bude měřena jejich výkonnost podle kritérií FAR (False Acceptance Rate) a FRR (False Rejection Rate). Na základě zjištěných poznatků a bude navrhnuta koncepce zabezpečení autentizace s využitím biometrické metody. Syntézou teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

3 Teoretická východiska

Teoretické části bakalářské se zakládá na analýze a rešerši odborných zdrojů. Dále bude analyzována autorizace do internetového bankovnictví u pěti největších bank (dle počtu klientů) v České republice.

3.1 Internetové bankovnictví

Internetové bankovnictví, dále internet banking je jedna z nejvyužívanějších forem přímého bankovnictví. Tutu službu nabízejí nejen Americké banky, tak i Evropské a Tuzemské banky. V český republice využívá internet banking již 5,5 milionů obyvatel (Cieslar, 2019) a počet stále roste.

Jako první banka, která v české republice začala nabízet internet banking byla už dnes neexistující banka Expandia, v té době klient mohl zadávat příkazy k úhradě, zakládat termínované vklady, získat informace o zůstatku na účtech, o posledních platbách, o kursech měn nebo úrokových sazbách.

V dnešní době má klient více možností a nabízených služeb jako například založení úvěru, založení dalšího účtu nebo založení a vedení investičního portfolia. Lze ale i přes internet banking měnit limity na kartě, nastavovat SIPO platby a trvalé příkazy a mnoho dalších věcí. Pro používání internet banking musí klient vlastnit počítač nebo jiné zařízení s přístupem na internet jako je Tablet a nainstalovaný webový prohlížeč nebo když je potřeba tak i bankou poskytovaný software. Internet banking je pro klienty, tak i pro banku výhodný druh přímého bankovnictví. Pro Klienty je internet banking levnější a dostupnější variantou Home Banking a především velkou úsporou času. Pro banky je Internet banking výhodný hlavně kvůli snížení nákladů na vlastní provoz.

(Švarc, 2001) (Internetové bankovnictví, c2011-2020) (Vejnar, 2001)

3.1.1 **Autentizace klienta v internetovém bankovnictví**

Internetové bankovnictví a všechny banky v české republice se řídí zákonem o bankovnictví č. 338/2020 Sb a regulací evropské unie PSD2(Payment Service Directive) a SCA(Strong Customer Authentication). (Global Payments Europe, 2019) (Zákony pro lidi, 2020)

Autentizace je proces, s nimiž se běžně setkává každý, kdo používá Internet banking. Většina veřejnosti není obeznámená co tento termín znamená a jak tento proces funguje. Průběh autentizace je zajišťovaný ze strany banky, která dbá tím to důraz na bezpečný přístup k internet bankingu uživatelem. (Miroslav, 2004)

Jde o proces, kdy dochází k určení uživatelovy identity, který přistupuje k systému – tedy zajišťuje, že daný systém ví, s jakým uživatelem komunikuje. Autentizaci je možní rozlišit do třech základních stupních dle (Rak, 2008) a (Matyáš, 2008)

A) Jednofaktorovou autentizaci
B) Dvoufaktorovou autentizaci
C) Třífaktorovou autentizaci

A) Jednofaktorová autentizace:

Nejméně bezpečná forma autentizace, která zahrnuje autentizaci klienta za pomoci uživatelského jména a hesla. Lze jí taky nazývat jako autentizaci znalostní.

Výhodou této autentizace je, že klient nepotřebuje k autentizaci žádný fyzický předmět, jde pouze o znalost, kterou klient může snadno používat kdekoliv a je snadno přenosná.

Nevýhodou této autentizace je, že utajovaná informace může být odhalena a následně zneužita nebo může být klientem zapomenuta. Jde tedy o nejméně bezpečnou formu autentizace. (Miroslav, 2004)

B) Dvoufaktorová autentizace:

Od jednofaktorové autentizace je dvoufaktorová autentizace rozdílná v tom, že již hraje roli více okolností. Nejde jen o využití abstraktních znalostí, ale dochází také k autentizaci za pomoci předmětu – identita se prokazuje vlastnictvím daného jedinečného předmětu. K přihlášení do internet banking je zapotřebí něco, co klient má, a nejen co zná. Předmětem vlastněný klientem může být například token nebo karta a znalostí klienta heslo nebo pin kód.

Výhodou dvoufaktorové autentizace je, že informace z tokenu (viz další strany bakalářské práce) lze velmi špatně odcizit nebo zkopírovat, protože tyto informace jsou zašifrované. Další výhodou, je řešení když dojde ke ztrátě Tokenu. Ztráta tokenu je velmi snadno zjistitelné a nálezce nemůže Token snadno použít a zneužít bez znalosti pinu či hesla. Dvoufaktorová autentizace je bezpečnější než Jednofaktorová.

Nevýhodou dvou faktorové autentizace je, že klient musí k Tokenu vlastnit příslušné čtecí zařízení, což sebou nese další pořizovací náklady při využívání tohoto zařízení. Další nevýhodou dvou faktorové autentizace patří ztráta, která je snadno zjistitelná, ale velmi špatně se vytváří náhradní přístroj, bez kterého se vlastník nedokáže autentizovat. Také může dojít k poruše zařízení, což se zjistí až při samotné autentizaci vlastníka. (Miroslav, 2004)

C) Třífaktorová autentizace:

Třífaktorová autentizace přidává k výše uvedenému druhu, tedy k, dvoufaktorové autentizaci ještě nějakou vlastnost či biologický znak klienta.

Výhodou této metody patří to, že každý má jedinečné znaky, které nelze nahradit nebo alespoň ne tak jednoduše. Další výhodou, je že klient tyto biometriky neztratí nebo nezapomene.

Nevýhodou této metody je, že informace odebírané z části těla jsou obtížně měřitelné, tak že přesnost měření může ovlivnit celkovou bezpečnost. Další nevýhodou je, nevratnost při poškození biometrického údaje. Příkladem, může být Diabetická retinopatie, která má za následek poškození nebo otoky sítnice, kdy klient nemusí být kvůli otoku sítnice

rozpoznán systémem. (Postižení oční sítnice může znamenat i trvalé poškození zraku (Ordinace.cz), 2014) (Matyáš, 2008)

Metody autentizace klienta do internetového bankovnictví

Mezi metody autentizace klienta do internetového bankovnictví patří dle (Matyáš, 2008)

A) Jméno a heslo
B) SMS kód
C) Certifikát
D) Kalkulátory
E) Čipové karty a tokeny

A) Jméno a heslo

Autentizace za pomoci Jména a hesla patří mezi nejrozšířenější metodu zabezpečení, lze jí považovat za základní způsob ověření identity a je vhodné jí kombinovat s další autentizací. Také je potřeba zdůraznit, že tato metoda je nejméně bezpečná ze všech metod zabezpečení, kvůli snadné infiltraci počítače a následné získání osobních či interních dat a informací.

Nevýhodou této metody je jednoduché odpozorování hesla. S tím je spojena i možnost využití Phishingu[1] či různých druhů Malwaru[2] útočníkem, které odhalí Jméno (login) a heslo.

Další možností odhalení jména a hesla je rozvoj techniky, hlavně rozvoj kamer, kdy útočník může nainstalovat malou bezdrátovou kameru oběti do obydlí.

Nejednoduší a nejelegantnější metodou získání *jména* a *hesla* uživatele je *přinucení* uživatele, aby použil pro přihlášení počítač útočníka, kde je nainstalovaný program sloužící k *odposlechu* stisku kláves na klávesnici.

Další nevýhodami této metody je zapomenutí jména nebo hesla, používání jednoduchého hesla, prozrazení hesla blízké osobě.

[1] Phishing-podvodná technika používaná na internetu k získávání citlivých údajů v elektronické komunikaci

[2] Malware-škodliví program, který v počítači provádí činnost, se kterou by uživatel nesouhlasil, kdyby o jeho skutečných záměrech věděl

Co se týče bezpečnosti je potřeba aby byli používaný taková hesla, které splňují podmínky silného hesla nastaveny bankou (každá banka má odlišné podmínky silného hesla) a aby byla zvýšená obezřetnost jak ze strany banky, tak i klienta.
Klient by měl, dostát i požadovaných bezpečnostních pokynů a dodržovat bezpečnostní desatero viz A Příloha. (Bitto, 2005) (Miroslav, 2004) (Matyáš, 2008)

B) SMS kód

Autentizace pomocí SMS (short message service) kódu je metoda autentizace, kdy je klientovy bankou vygenerovaný jednorázový heslo s časovou lhůtou, a to je odesláno na příslušní číslo, které uvedl klient banky při zakládání bankovního účtu. (Matyáš, 2008)

C) Certifikát

Autentizace pomocí certifikátu je druh autentizace, kdy banka vydá časově omezený certifikát, který je použit při ověření žádosti o autentizaci.
Tento certifikát obsahuje příslušný soukromý klíč a nachází se většinou na externím paměťovým mediu jako například disketa – dnes už zastaralé a nepoužívané medium nebo flashdisk.
Tato metoda je málo bezpečná proto, že většina klientů už dál nepoužije další jiný způsob zabezpečení počítače, například *firewall*, který by fungoval jako další bezpečnostní prvek mezi útočníkem a uživatelem. (Miroslav, 2004) (Matyáš, 2008)

D) Kalkulátory

Kalkulátory rozdělujeme na dva druhy.
Jedním z nich jsou kalkulátory bez PIN(Personal Identification Number), které jsou velice rizikové, kvůli tomu, že neexistuje u nich žádný ochranný prvek, který by zaručoval nemožnost zneužití při ztrátě uživatelem nebo odcizení útočníkem.
Druhý druh kalkulátoru je tak zvaný kalkulátor chráněný PIN kódem, který je bezpečnější než kalkulátor bez PIN kódu. Kalkulátor chráněný PIN kódem je zabezpečený algoritmem, který je velmi těžce prolomitelný, a proto při ztrátě nebo odcizení útočníkem je malá pravděpodobnost zneužití. (Ludvík, 2004) (Matyáš, 2008)

E) Čipové karty a tokeny

Čipové karty a tokeny patří mezi jedny z nejbezpečnějších variant autentizace do internetového bankovnictví.

Jsou zabezpečený PIN kódem a, nebo kódem nazývaný PUK(Personal Unlocking Key) (některé banky nabízejí mobilní tokeny, které jsou zabezpečené PIN kódem nebo biometrií), který uživatel musí zadat vždy při práci se systém.

Metoda autentizace využívá obecně známé šifrovací algoritmy a standardy.

U některých tokenů, lze najít ještě tak zvaný certifikát na obal, který zabezpečuje zničení všech uložených operací a rozpadnutí obalu při pokusu rozebrání tokenu útočníkem. (Ludvík, 2004) (Matyáš, 2008)

3.1.2 Přehled metod autentizace klienta u vybraných bank

Každá banka nabízí jiné možnosti autentizace klienta do internet banking.

V této kapitole si představíme pět největších bank v české republice podle počtu klientů a jejich nabídku autentizace klienta do Internet banking. (Hovorka, 2020)

Česká Spořitelna

Jedna z největších komerčních bank založená 12. února roku 1825 v České republice s nejdelší tradicí na českém trhu.

Od roku 2000 je součástí rakouské skupiny Erste Bank, která eviduje 16.1 milionů klientů a z toho 4,6 milionů klientů patří České spořitelně.

Česká spořitelna využívá metody autentizace, které jsou uvedeny v Tabulka 1.

(Česká spořitelna Všeobecná prezentace o Finanční skupině ČS, 2020) (Kdo jsme, 2020)

Tabulka 1 Metody autentizace klienta do internetového bankovnictví u České spořitelny

Metody autentizace klienta do internetového bankovnictví u České spořitelně	
Uživatelské Jméno/Klientské číslo	✓
Heslo	✓
SMS	✓
Certifikát	✗
Kalkulátor	✗
Čipová karta	✗
Token	✓

Zdroj: (Česká Spořitelna, 2020)

ČSOB

Československá obchodní banka a.s je stoprocentní dceřinou společnostní KBC Bank VC a v České republice působí jako univerzální banka.

ČSOB založil stát roku 1964 jako banku pro poskytování služeb financování zahraničního obchodu a volno měnových operací.

Po roce 1999 byla banka privatizována a jejím majoritním vlastníkem se stala KBC bank. O rok později v roce 2000 převzala investiční a poštovní banku IPB.

ČSOB eviduje 4,241 milionu klientů v České republice.

ČSOB využívá metody autentizace, které jsou uvedeny v Tabulka 2.

(O ČSOB a skupině, 2020)

Tabulka 2 Metody autentizace klienta do internetového bankovnictví u ČSOB

Metody autentizace klienta do internetového bankovnictví u ČSOB	
Uživatelské Jméno/Klientské číslo	✓
Heslo/PIN	✓
SMS	✓
Certifikát	✗
Kalkulátor	✗
Čipová karta	✓
Token	✓

Zdroj: (ČSOB, 2018)

Komerční banka

Komerční banka vznikla roku 1990 kdy byla vyčleněná obchodní část z bývalé státní Československé banky.

V roce 2001 byla prodaná francouzské Société Générale, která vyzdvihla komerční banku jak na prahu služeb, tak technologií.

Komerční banka eviduje 1,67 milionu klientů.

Komerční banka využívá metody autentizace, které jsou uvedeny v Tabulka 3.

(Historie KB, 2020) (Fakta a výsledky, 2020)

Tabulka 3 Metody autentizace klienta do internetového bankovnictví u Komerční banky

Metody autentizace klienta do internetového bankovnictví u Komerční banky	
Uživatelské Jméno/Klientské číslo	✓
Heslo	✓
SMS	✓
Certifikát	✓
Kalkulátor	✗
Čipová karta	✓
Token	✓

Zdroj: (KB, 2020)

Moneta

Moneta Money Bank byla založena v roce 1998 pod názvem GE Capital Bank na českém trhu. V roce 2008 prošla bankou vizuální změnou a stala se zní GE Money Bank.

V roce 2016 v stupuje banka na Burzu a společnost GE prodává veškerá své finanční divize. Tím to rokem se stala ryze českou bankou pod názvem Moneta Money Bank.

Moneta Money Bank eviduje 0,99 milionu klientů.

Moneta Money Bank využívá metody autentizace, které jsou uvedeny v Tabulka 4.

(Historie MONETA Money Bank, 2020) (Bureš, 2020)

Tabulka 4 Metody autentizace klienta do internetového bankovnictví u Monety

Metody autentizace klienta do internetového bankovnictví u Moneta Money Bank	
Uživatelské Jméno/Klientské číslo	✓
Heslo	✓
SMS	✓
Certifikát	✓
Kalkulátor	✗
Čipová karta	✗
Token	✓

Zdroj: (Moneta money bank, 2020)

Fio banka

Banka byla založena v roce 1993 a zaměřovala se na obchodování s cennými papíry.

Jako první v roce 1998 spustila Internetové bankovnictví z dnešních finančních institucí v české republice. V roce 2006 banku koupila firma RM-systém a následně v roce 2010 získává Fio banka bankovní licenci. Fio banka eviduje 0,98 milionu klientů. Fio banka využívá metody autentizace, které jsou uvedeny v Tabulka 5.

(Historie, 2020) (Bureš, 2020)

Tabulka 5 Metody autentizace klienta do internetového bankovnictví u Fio banky

Metody autentizace klienta do internetového bankovnictví u Fio banky	
Uživatelské Jméno/Klientské číslo	✓
Heslo	✓
SMS	✓
Certifikát	✗
Kalkulátor	✗
Čipová karta	✗
Token	✓

Zdroj: (Fio banka, 2020)

3.2 Využití biometrie pro zabezpečení

Slovo biometrie vzniklo spojením řeckých slov BIO-život a METRIC-měření a je definováno jako „obor zabývajícího se použitím matematické statistiky pro zkoumání proměnlivosti živých organismů (Černohorský, 2003). Každé lidské tělo je unikátní a lze na něm pozorovat nebo najít mnoho jedinečných znaků, které lze využít jako rozpoznávací znamení. Například jen na hlavě můžeme použít sken oční duhovky, obličeje, sítnice oka, tvar ucha nebo náš hlas, na těle pak otisk prstu, geometrie dlaně, lidský pach, obsah soli v lidském těle, dynamiku stisku klávesy na klávesnici a mnoho dalších.

Znaky rozdělujeme do dvou skupin biometrických charakteristik, a to Behaviorální biometrické charakteristiky a Anatomicko-fyzikální biometrické charakteristiky. (Bitto, 2005) (Rak, 2008)

3.2.1 **Behaviorální biometrické charakteristiky**

Behaviorální biometrická identifikace je založena na základě zkoumání specifických rysů chování Člověka. Behaviorální biometrická charakteristika pracuje s poznatky o lidském hlase, pohybu těla, dovednostech a znalostech psaní rukou.

Mezi behaviorální charakteristiky, teda charakteristiky týkajících se chování člověka řadíme psaní souvislého textu, dynamiku stisku kláves na klávesnici a dynamiku podpisu osoby. (Bitto, 2005)

„Behaviorální biometrické charakteristiky jsou unikátní a můžou být časově nestále“ (Rak, 2008).

Identifikace hlasem

Hlas neboli hlasový signál je výsledek aktivity neuromuskulárních příkazů, které vytlačují vzduch z plic, který má za následek vibraci nebo klid hlasových chord a formují hlasový trakt.

V biometrických technologiích se ověřovaní hlasu zakládá na rozdílnostech vokálních traktů jednotlivých osob, kde tvar a rezonance ústní dutiny, jazyka a zubů, hlasivek jednoznačně formuje biometrický otisk každé osoby. Identifikace hlasu se používá od sedmdesátých let dvacátého století a neustále se zdokonaluje a je kladen důraz na její zkoumání.

Rozpoznávání hlasu a ověřování hlasu jsou zcela dva odlišné přístupy zkoumaní hlasu. Při rozpoznávání hlasu musí daná osoba vyslovit slovo, které následně systém vyhledá v databázi a určí, zda slovo se shoduje s danou výslovností. Opačným přístupem je ověřování osoby za pomocí hlasu. Při ověřování hlasu osoby se porovnává fráze vyslovená osobou s registrovaným vzorkem osoby nahraným dříve do databáze, kdy posléze systém určí míru shody mezi vyslovenou frází osoby a registrovaným vzorkem. Nevýhodou při rozpoznávání hlasu je, že systém dokáže určit, co bylo vysloveno, ale nikoliv kdo to vyslovil.

(Bitto, 2005) (Rak, 2008)

Průběh při identifikaci hlasu:

1) Při registraci každá osoba nahraje svůj vzorek hlasu tzv „otisk hlasu“. Pro lepší bezpečnost osoba nahraje delší namluvené slovo nebo větu a tím je zaručen větší stupeň bezpečnosti. (Bitto, 2005)

2) V průběhu identifikace je člověk pobídnut, aby vyslovil svou větu nebo slovo. Vyšší bezpečnost poskytují systémy, které při registraci vyžadují několik různých frázích a při identifikaci náhodně vyberou jen jednu z nich. (Bitto, 2005)

3.2.2 **Anatomicko-Fyziologické biometrické charakteristiky**

Anatomicko-fyziologické biometrické charakteristiky využíváme pro identifikaci nebo verifikaci osob na základě vědeckých poznatků Anatomicko-fyziologických vlastnostech člověka. Mezi anatomicko-fyziologické charakteristiky patří vědecké poznatky o oční sítnici, oční duhovce, tváři, otiscích prstů, dlaně a chodidel, stavbě vnějšího ucha, geometrie prstů a ruky, lidském tělesném pachu, topografie žil zápěstí, obsahu soli v lidském těle, rozměrech a váhách lidského a skladbě DNA.
„Anatomicko-fyziologické biometrické charakteristiky jsou časově stálé a unikátní“. (Bitto, 2005) (Rak, 2008)

Identifikace otiskem prstu

Otisk prstu je jedna z nejpoužívanějších a nejznámějších biometrických metod a zároveň nejstarší metoda identifikace, používaná ve forenzní sféře.
Povrch prstu je tvořený drobnými prolákliny a vyvýšeninami, které vznikli vybíháním škáry proti pokožce tzv papilách. Jan Evangelista Purkyně klasifikoval devět základní vzorů papilárních liniích.

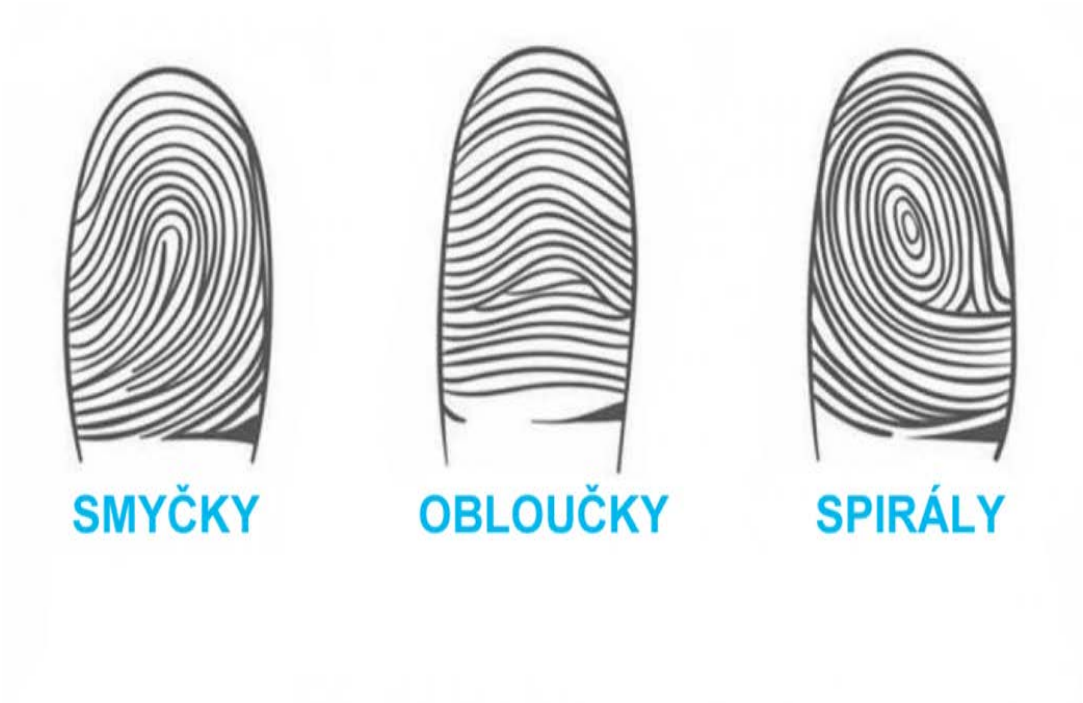
V novodobý klasifikaci jsou rozeznávaný tři základní vzory a to oblouk, vír, smyčka (Obrázek 1).

Oblouk: tento vzor neobsahuje žádné delty[3] a papilární linie vytvářejí jednoduché oblouky.

Vír: tento vzor obsahuje alespoň dvě delty a papilární linie vytvářejí oválné, kruhové nebo spirálovité obrazce s jádrem ve středu.

Smyčka: tento vzor obsahuje alespoň jednu probíhající linií mezi deltou a středem. Papilární linie tvoří smyčky.

Obrázek 1 Tři základní vzory papilárních liniích



Zdroj: (Kovanda, 2018)

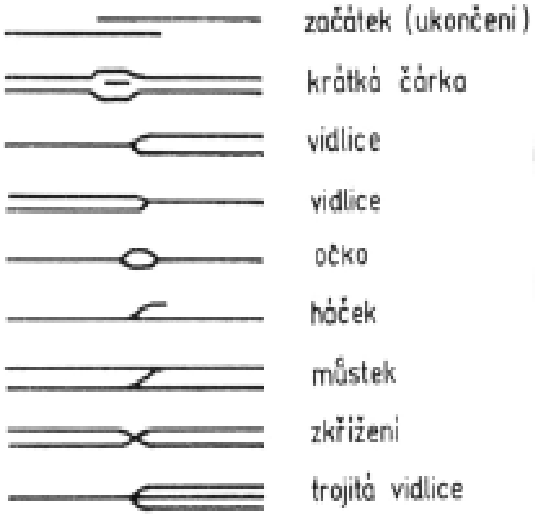
Vlastní identifikace je založena na objevení a porovnání významných znaků tzv. Markantů[4], které papilární linie tvoří. Rozeznáváme ty to základní druhy markantů: body, ostrůvky,

[3] Delty tj. útvary v nich se papilární linie rozbíhají do tří směrů.
[4] Markanta-jakákoliv změna v průběhu papilární linie, která se odlišuje od ostatních.

zdvojení, háček, očko, posunutí, křížení, tečka, krátká linie, trojitá vidlice, začátek a konec linie, můstky a další (Obrázek 2).

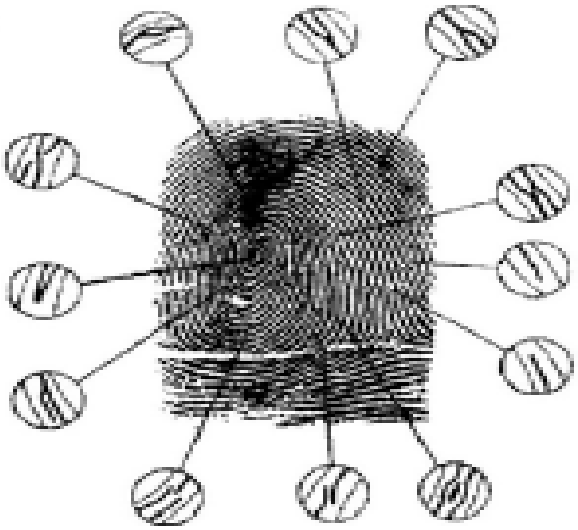
Na otisku prstu lze nalézt 75-175 markantů, z toho některý jsou častěji vyskytující než jiné (Obrázek 3). (Rak, 2008) (Bitto, 2005)

Obrázek 3 Základní druhy markantů



Zdroj: (Slaninová, 2019)

Obrázek 2 Vyznačené markanty na otisku prstu



Zdroj: (Slaninová, 2019)

Druhy snímačů otisku prstu:

a) Optoelektronické biometrické snímače

Tento druh snímače je převážně vhodný pro algoritmy rozpoznávání založených na markantech. Princip pracování je založený na rozdílech odrazu světla.

Optický snímač zachytí digitální zobrazení otisku prstu pomocí viditelného světla a obraz přenese na maticový CCD(Charge Coupled Device) detektor, který následně je digitalizován a předán dál na zpracování. (Biometrie otisku prstu, c2011-2020), (Čtečky otisků prstů v mobilech: typy a funkce, 2020)

Výhody: minimální vliv okolního prostředí, vysoká kvalita

Nevýhody: při znečistění nebo poškození prstu zařízení nedokáže dobře vykreslit obraz prstu.

Obrázek 4 Optický snímač otisku prstu

Zdroj: (Beňovič, 2020)

b) Kapacitní biometrické snímače

Tento druh snímače lze nalézt na mnoho chytrých mobilních telefonech, kde slouží jako bezpečnostní prvek zabezpečení telefonu, před neautorizovanými uživateli.

Princip pracování je založený na využití rozdílu kapacity mezi deskou snímače a povrchem prstu, kdy papilární linie mají vyšší kapacitní odpor než mezery mezi nimi. (Biometrie otisku prstu, c2011-2020), (Čtečky otisků prstů v mobilech: typy a funkce, 2020), (Otisk prstu, 2020)

Výhody: vysoká kvalita, malý rozměr

Nevýhody: krátká doba životnosti

c) Teplotní biometrické snímače

Princip pracování je založený na snímání rozdílů teplot mezi jednotlivými papilárními liniemi a prostory mezi nimi. K měření se používá citlivý čip pyrodetektor[5]. (Biometrie otisku prstu, c2011-2020), (Otisk prstu, 2020)

Výhody: žádná

Nevýhody: nízká kvalita, problémy s Algoritmy zpracovávající markanty

[5] Pyrodektor-pasivní infračervené čidlo

d) Elektroluminiscenční biometrické snímače

Princip zpracování je založený na využití vrstvy, která reaguje na tlak způsobený luminiscenčním efektem. Zpracování je zajištěno fotodiodou. (Biometrie otisku prstu, c2011-2020), (Otisk prstu, 2020)

Výhody: miniaturní rozměry
Nevýhody: náchylnost vůči znečištění

e) Radiofrekvenční biometrické snímače

Princip zpracování je založený na připojení generátoru střídavého signálu k, dvěma rovnoběžným deskám (plocha snímače a plocha otisku prstu). (Biometrie otisku prstu, c2011-2020), (Otisk prstu, 2020)

Výhody: velká odolnost vůči znečištění a nečistotě otisku prstu
Nevýhody: žádná

f) Ultrazvukový biometrické snímače

Princip zpracování je založen na technologie ultrazvuku, kdy
zařízení je vybaveno ultrazvukovým přijímačem a vysílačem, který vysílá signál k prstu a ten se zpět od prstu odráží k přijímači. Přijímač dále vyhodnocuje časovou posloupnost vrácených odrazů. Jedná se o nejmodernější typ čtečky otisků prstů. (Čtečky otisků prstů v mobilech: typy a funkce, 2020),
(Biometrie otisku prstu, c2011-2020)

Výhody: vysoká přesnost snímání
Nevýhody: vysoké výrobní náklady

Identifikace tváří

S touto metodou identifikace se setkáváme každý den a je naší denní rutinou, ačkoliv si to ani neuvědomujeme, každý rozeznává lidi podle obličeje. Lidský obličej obsahuje až 80 typických rysů a k jeho rozeznání nám stačí diagnostikovat pouze 14 – 20 z nich.

K rozeznání tváře za pomocí počítače se používá několik algoritmů, z nichž nejpoužívanější jsou srovnání podle šablon a měření geometrie obličeje.
Technika srovnávání šablon funguje na principu porovnání právě pořízené šablony obličeje uživatele s referenční šablonou uživatele uloženou v databázi. V databázi se nachází mnoho šablon obličejů, kdy při srovnání se určuje jejich míra podobnosti s právě pořízenou šablonou.

Technika rozeznání tváře za pomocí měření geometrie obličeje funguje na principu určování pozic význačných částí obličeje a měření vzdáleností mezi nimi. Význačné časti obličeje jsou například nos, oči, ústa, obočí.

Fáze identifikace obličeje dle (Bitto, 2005) a (Rak, 2008):

1) Detekce obličeje – Systém prochází obraz a hledá tvar hlavy. Nejvýznamnější algoritmů pro hledání obličeje je tak zvaný „klouzající okno“. Rychlost detekce obličeje může ovlivnit například nevhodné pozadí.

2) Úprava obrazu – po rozeznání obličeje, software obličej upraví natočením, zvětšením či zmenšením do požadované velikosti.

3) Vytvoření šablony – Algoritmus zakóduje obraz obličeje do šablony.

4) Porovnání šablon – Právě vytvořená šablona je porovnávána s prvky databáze a je určena míra schody a z ní stanoven výsledek identifikace.

3.2.3 **Kritéria pro biometrické technologie**

Kritéria pro biometrickou technologii používáme při zhodnocení biometrické technologie pro praktické a efektivní nasazení, tak i pro samotnou funkčnost biometrických identifikačních a verifikačních technologií. Kritériích pro biometrickou technologii je mnoho, některý odrážejí ekonomičnost, praktičnost nebo společenskou a finanční přijatelnost. Jiné jsou spojeny se základní teorií a praxí. Kritéria pro biometrickou technologii rozděluje podle určitých společných a typických znaků do skupin: Operační Kritéria, Matematická, algoritmická a bezpečnostní kritéria, Technická kritéria, finanční kritéria a výrobní kritéria. (Rak, 2008)

Operační kritéria

Do skupiny operačních kritéria patří dle (Rak, 2008) následující charakteristiky:

- **Jedinečnost** – biometrické charakteristiky dané identifikační metody musí být unikátní, aby bylo možné přesně a spolehlivě rozeznat jednu osobu od druhé.

- **Neměnnost** – prvky, na kterých staví biometrická identifikace musí být stále a časově neměnné.

- **Měřitelnost** – charakteristiky, na niž je založená identifikace musí být měřitelné a musí být symbolicky vyjádřitelné.

- **Uchovatelnost** – naměřené identifikační charakteristiky musí být možné archivovat s akceptovatelnými náklady na kvalitu archivace, aby nedošlo ke ztrátě kvality nebo poškození.

- **Spolehlivost** – proces zpracování, měření a ukládání musí být spolehlivý a kdykoliv zopakovatelný s totožnými výsledky.

- **Exkluzivita** – identifikační metoda by měla být úplná (dostačující) aby nebyla potřeba další identifikační činnost.

- **Praktičnost** – metoda identifikace musí být praktická. Uživatel by měl při procesu identifikace ztratit co nejmíň času, měření by mělo být co nejednoduší, uživatel by se měl dostat do minimálního kontaktu s technologickým zařízením a vyžadovat minimum tréninku uživatele.

- **Přijatelnost** – Proces snímání a vyhodnocování by měl být nerušiví a u osoby by neměl vyvolávat pocity diskriminace např: barvou pleti, věkem, profesí, fyzickým nebo psychologickým stavem.

- **Uživatelská přívětivost** – Proces vyhodnocování a snímaní nesmí být rušiví nebo vtíravý a uživatele nesmí diskriminovat nebo rušit při snímaní.

Matematická, algoritmická a bezpečnostní kritéria

Biometrické metody používají mnoho různých kódů, matematických algoritmů, kompresy a protokoly.

Biometrické matematické algoritmy rozdělujeme dle (Rak, 2008) do tří kategorií:

- Statické metody modelování
- Dynamické programování
- Neuronové sítě

Každý algoritmus musí být před použitím řádně otestován, ohodnocen a certifikován specialistou, aby nedocházelo k nasazení chybného nebo děravého algoritmu.

Různé algoritmy nabízejí různé stupně bezpečnosti. Čím víc je potřeba vynaložit úsilí na překonání algoritmu tím je algoritmus bezpečnější.

O technologické kvalitě používané metody nerozhodují jen algoritmy, ale i kódování, protokoly a databáze. Je dbán velký důraz na jejich bezpečnost a spolehlivost.

Při hodnocení metodologických, bezpečnostních a algoritmických kritérií se dle (Rak, 2008) posuzuje:

- Správnost teorie
- Správnost algoritmů
- Bezpečnost protokolů
- Bezpečnost síťového a distribuovaného prostředí
- Bezpečnost algoritmů
- Správnost výběru markantů (klíčů, identifikačních markantů)
- Zabezpečení databáze s biometrickými údaji
- Efektivita a zabezpečení kódování biometrických údajů

Technická Kritéria

Mezi nejvíce používaná vyhodnocovací kritéria v oblasti biometrické identifikace patří dle (Rak, 2008) tyto charakteristiky:

- Minimální čas zpracování/vyhodnocení identifikačních charakteristik
- Přijatelná chybovost
- Flexibilita
- Odolnost
- Efektivnost
- Výkonost
- Standardizace
- Skladovatelnost identifikačních charakteristik
- Požadovaná prostor na uložení a zpracování identifikačních charakteristik, velikost šablony
- Přesnost
- Jednoduchost
- Rychlost
- Nezávislost na vnějším prostředí

Finanční kritéria

Finanční otázka hraje velkou roli při vývoji a nákupu biometrických technologií.
Finanční stránka se hodnotí jak z pohledu jednorázového nákupu, tak i z pohledu dlouholetého provozu.

Zohledňují se dle (Rak, 2008) tyto kritéria:

- Cena instalace
- Náklady spojené s uvedením do provozu
- Pořizovací cena technologie
- Cena následujících upgradů
- Cena návazných systémů
- Cena logistické podpory a provozu
- Cena dalších zamýšlených zařízení
- Cena obsluhy zařízen

Výrobní kritéria

Při výběru je důležité zohlednit kvalitu dodavatele, výrobce technologií a také cenu a efektivnost podpory při provozu zařízení ze strany dodavatele nebo výrobce. Dále je důležité myslet na kontabilitu s budoucími technologiemi nebo technologiemi už zavedenými a referencemi od dalších uživatelů. (Rak, 2008)

3.3 Měření výkonosti biometrických metod a zařízení

U každého zařízení nebo metody lze měřit, zda je dostatečně výkonné nebo spolehlivé pro verifikaci nebo identifikaci Osoby. Toto měření vyjadřujeme ve dvou kritérií a FRR (False Rejection Rare) můžeme se setkat i s označením chyba 1.typu a FAR (False Acceptance Rate**)** označovaným taky jako chyba 2.typu. (Rak, 2008) (Bitto, 2005)

3.3.1 **Pravděpodobnost chybného odmítnutí**

Pravděpodobnost chybného odmítnutí FRR je jedním z kritérií ukazující uživatelskou a bezpečnostní spolehlivost. Udává pravděpodobnost, že biometrické zařízení bude chybovat a nerozpozná oprávněného uživatele nebo dříve registrovanou osobu, která má v aplikaci uloženou svou referenční biometrickou šablonu.
Důsledkem je pak tento uživatel odmítnut a musí se znovu pokusit o prokázání své identity. (Rak, 2008) (Bitto, 2005)

Pravděpodobnost chybného odmítnutí můžeme definovat podle (Rak, 2008) jako

Rovnice 1 Pravděpodobnost chybného odmítnutí

$$FRR = \frac{N_{FR}}{N_{ELA}} \quad \text{nebo} \quad FRR = \frac{N_{FR}}{N_{EVA}}$$

FRR-pravděpodobnost chybného odmítnutí
N_{FR}-počet chybných odmítnutí
N_{ELA}-počet pokusů oprávněných osob o identifikaci
N_{EVA}-počet pokusů oprávněných osob o verifikaci

FRR lze vyjádřit i graficky za pomoci histogramu jako poměr dvou ploch (Rak, 2008):

Rovnice 2 Pravděpodobnost chybného odmítnutí jako poměr dvou ploch

$$FRR = \frac{P_{A,B,E,A}}{P_{A,B,C,D,A}}$$

3.3.2 **Pravděpodobnost chybného přijetí**

Pravděpodobnost chybného přijetí FAR udává pravděpodobnost, že biometrické zařízení bude chybovat a přijme neoprávněného uživatele nebo neregistrovanou osobu. Důsledkem je pak umožnění přístupu neregistrovaní nebo neoprávněný osobě. (Rak, 2008) (Bitto, 2005)

Pravděpodobnost chybného přijetí můžeme definovat podle (Rak, 2008) jako

Rovnice 3 Pravděpodobnost chybného přijetí

$$FAR = \frac{N_{FA}}{N_{IIA}} \text{ nebo } \quad FAR = \frac{N_{FA}}{N_{IVA}}$$

FAR-pravděpodobnost chybného přijetí

N_{FA}-počet chybných přijetí

N_{IIA}-počet pokusů neoprávněných osob o identifikaci

N_{IVA}-počet pokusů neoprávněných osob o verifikaci

FAR lze vyjádřit i graficky za pomoci histogramu jako poměr dvou ploch (Rak, 2008):

Rovnice 4 Pravděpodobnost chybného přijetí jakopoměr dvou ploch

$$FAR = \frac{P_{W,X,EW}}{P_{U,V,X,U}}$$

4 Vlastní práce

Praktická část bakalářské práce se zabývá zhodnocením tří biometrických metod, a to Otiskem prstu, Tváří a Hlasem podle kritérií pro biometrické metody dle (Rak, 2008). Dále se věnuje návrhem tří fázové autentizace s využitím biometrické metody dle hodnocení tří vybraných biometrických metod.

4.1 Verifikace otiskem prstu

Otisk prstu je nejvíce využívanou biometrickou metodou sloužící k verifikaci uživatele. Techniky využívající biometrickou metodu otisk prstu je po celém světě hodně a stává se nejdostupnější biometrickou metodou, lze jí nalézt na mobilních telefonech, tabletech, notebucích, přenosných paměťových medií a klávesnicích.

4.1.1 Zhodnocení z hlediska operačních kritérií

Jedinečnost – každý otisk prstu není jedinečný a pravděpodobnost schody je 1:1000000.
Neměnnost – markanty nacházející se na prstu jsou neměnné po celý život uživatele.
Měřitelnost – biometrickou metodu lze měřit více druhy senzorů a to kapacitním, teplotním, ultrazvukovým a dalšími. Metoda je dostupně měřitelná.
Uchovatelnost – naměřenou biometrickou hodnotu lze archivovat bez její degradace nebo poškození.
Spolehlivost – biometrická metoda se blíží spolehlivosti a lze jí zopakovat se stejnými výsledky. Ale není dostatečně spolehlivá. Při úmyslném poškození nelze naměřit stejný výsledek jako při prvním měření.
Exkluzivita – při identifikaci otiskem prstu nemusí být použita další pomocná identifikační metoda, ale nejedná se o sto procentní exkluzivitu. Při velkém poškození otisku prstu uživatele musí být už dodatečně použitá další identifikační metoda.
Přijatelnost – uchování, zpracování a vyhodnocování je přijatelné ze všech hledisek a to osobního, náboženského, etického, politického, společenského.
Praktičnost – biometrická metoda otisk prstu je praktická. Při identifikaci uživatel provádí jen jeden úkon a nemusí podstupovat žádný trénink, jak používat čtečku nebo jak sní pracovat.

Rychlost verifikace je ovlivněná použitým systém a typem snímače. V dnešní době trvá autentizace uživatele v řádku vteřin.
Uživatelská přívětivost – biometrická metoda otisku prstu je přívětivá. Při snímaní neruší uživatele a ani při vyhodnocování. Při špatném zvolení použití v prostředí, může diskriminovat uživatele (například při použití v prostorách s nutností nošení ochranného obleku).

4.1.2 **Zhodnocení z hlediska výrobních kritérií**

Biometrická metoda otisk prstu je nejvíce rozšířenou a dostupnou metodu zabezpečení v dnešní době. Většina výrobců implementuje do zařízení technologii využívající kapacitní senzor, kde rozdíl mezi těmi to senzory je už zanedbatelný.
Liší se jen malým nebo žádným rozdílným počtem kondenzátorů a použitým softwarem. Lze nalézt i výrobce co do svých zařízení implementují senzory optické a ultrazvukové, ale nejsou tak rozšířené jako senzory kapacitní. Proto není důležité dávat takový důraz při výběru zařízení z hlediska druhu senzoru v zařízení.
Mnoho výrobců ani neuvádí v technických specifikacích, o jaký druh senzoru se jedná. Důležité je ale zaměřit se na samotnou podporu ze strany výrobce a zhodnotit ty to tři hlediska: Podpora řešení problémů, délka podpory aktualizací softwaru a kompatibilita s jinými zařízení. Když zhodnotíme biometrickou metodu otisk prstu z hlediska kompatibility, vyjde, že díky sví rozšířenosti se jedná o nejvíce kompatibilní metodu.
Z hlediska podpory řešení problémů a délky podpory aktualizací, záleží na výrobci, a proto bych doporučil vybírat výrobce podle garance těchto, dvou služeb.

4.1.3 **Zhodnocení z hlediska matematických, algo. a bezpečnostních kritérií**

Každý výrobce čtečky otisků prstů dodává s hardwarem i svůj vlastní software, který je před nasazením otestován a o certifikován a tím výrobce zabezpečuje i jeho samotnou bezpečnost. Z hlediska samotné metody už otisk prstu není tak bezpečný, kvůli jednoduchému zanechání na předmětech jako je například sklenička, klika od dveří a další.

Proto se metoda stává z hlediska bezpečnosti velmi nebezpečná a záleží, zda čtečka otisků prstů disponuje další technologii, která rozeznává, zda se jedná doopravdy o prst uživatele nebo jen napodobeninu nosící identifikační prvky (markanty).

4.1.4 **Zhodnocení z hlediska technických kritérií**

Z hlediska technických kritérií trh nabízí mnoho řešení. A proto je důležité, aby si uživatel nastavil standarty podle kritérií, který si sám zvolí jako důležité. Čtečky otisků prstů a zařízení s čtečkou otisků prstů jsou náchylné na rozbití. Z pohledu uživatele je důležité, aby se uživatel zaměřil na použitou technologii u čtečky otisků prstů viz teoretická rešerše bakalářské práce. A zda čtečka disponuje i další bezpečnostní technologií, která zajistí, zda se skutečně jedná o prst uživatele nebo falzifikát.

4.1.5 **Zhodnocení z hlediska finančních kritérií**

Zařízeních, které mají integrovanou čtečku otisků prstu je na trhu mnoho, a proto je biometrická metoda otisk prstu nejdostupnější biometrickou metodou sloužící jako bezpečnostní prvek. Dle cenového rádce Heuréka lze nejlevnější tablet se čtečkou otisku prstu koupit už za 8 893 Kč a nejlevnější notebook za 6 489 Kč, cena se ale pak i hodně odráží v kvalitě, bezpečnosti a použitelnosti zařízení. Proto je dobré držet se při výběru technických a výrobních kritérií. Trh nabízí i externí čtečky otisků prstu, které lze připojit k zařízení. Zde se cena pohybuje od 1 207 Kč do 7 932 Kč. Cena se, ale hodně odráží v kvalitě a použité technologii. Dražší čtečky otisků prstů jsou kvalitnější a disponují další technologií určenou k rozpoznání, zda se jedná o falsifikát otisku prstu nebo skutečný otisk prstu uživatele.

4.1.6 **Zhodnocení FRR a FAR**

Hodnota FRR u otisku prstu je často udávána 0,1 % a hodnota FAR 0,001% (Fujitsu Limited, 2012) .

Z hodnoty FAR vidíme, že systém používající k autentizaci biometrickou metodu otisk prstu přijme 0,001% neoprávněných uživatelů a z hodnoty FRR vidíme, že systém neoprávněně odmítne 0,1 % uživatelů s oprávněním.
Ideální zařízení nebo aplikace nevykazuje žádnou nespolehlivost nebo chybovost, když hodnota FAR a FRR se rovná nule neboli platí vztah, že FRR=FAR=0. (Rak, 2008) U zařízení nebo aplikací využívající biometrické metody otisk prstu lze pozorovat, že naměřené hodnoty se sice blíží k nule, ale pořád se nejedná o ideální zařízení, které by nevykazovalo chyby a bylo stoprocentně spolehlivé.

Ty to hodnoty jsou nejčastější naměřené, ale orientační a jsou ovlivňovány nastavením vstupního citlivostního prahu.

4.2 Verifikace tváří

Verifikace obličejem je jedna z nejčastějších identifikačních metod, používaná už od samotného počátku lidstva. Kdy člověk identifikoval jiného člověka podle tváře, kterou si zapamatoval. Jedná se o nejpřirozenější biometrickou metodu. V dnešní době jí lze nalézt jako bezpečnostní prvek na mobilních telefonech, tabletech, notebucích nebo na letištích sloužící k identifikaci člověka.

4.2.1 Zhodnocení z hlediska operačních kritérií

Jedinečnost – nejedná se o jedinečnou biometrickou metodu. Příkladem můžou být jednovaječná dvojčata, kdy rysy obličeje jsou stejné nebo podobné a je potřeba k rozeznání více rysů.
Neměnnost – lidská tvář se časem a životosprávou mění a proto, je neměnnost u této biometrické metody velmi špatná.
Měřitelnost – biometrickou metodu lze měřit opticky nebo infračerveně.
Uchovatelnost – naměřenou biometrickou hodnotu lze archivovat bez její degradace nebo poškození. Ale je nutné jí kvůli měnivosti lidské tváři časem často obnovovat.

Spolehlivost – proces zpracování a ukládání je spolehlivý díky technologii a vyspělosti kamerových systémů a samotných kamer.

Exkluzivita – identifikační metoda je exkluzivní a není potřeba další dodatečné měřící metody.

Přijatelnost – biometrická metoda je přijatelná. Osoby neruší a nevyvolává pocity diskriminace.

Praktičnost – biometrická metoda je praktická. Osoba u ní neztratí žádný čas a nevyžaduje žádný trénink uživatele.

Uživatelská přívětivost – biometrická metoda je uživatelsky přívětivá. Osobu neruší a není vtíravá. Při snímaní osobu neruší a nediskriminuje.

4.2.2 Zhodnocení z hlediska výrobních kritérií

Z hlediska výrobních kritérií je třeba zvážit a zaměřit se na samotnou podporu a budoucí kompatibilitu a použitý algoritmus. Samotný trh nenabízí mnoho řešení a řešení jsou u mnoho případů hodně nákladné, ale jsou stavěny nebo přizpůsobovány na míru. Z pohledu uživatele je pak důležité, aby uživatel disponoval kvalitním hardwarem.

4.2.3 Zhodnocení z hlediska matematických, algo. a bezpečnostních kritérií

Verifikace obličejem používá mnoho algoritmů, z nichž nejznámější je měření geometrie obličeje a srovnávání šablon, klouzající okno viz teoretická část bakalářské práce.

Tyto algoritmy byli řádně otestovány společnostmi, která je používají ve svých zařízení a jsou řádně certifikovány dodavateli.

4.2.4 Zhodnocení z hlediska technických kritérií

Z hlediska technických kritérií trh nenabízí už skoro žádné zařízení, které by nedisponovalo webkamerou o rozlišení nejmíň 2 MPx(Mega pixel) a nebylo jednoduché na použití. Zařízení, ale nejsou moc odolná a jsou závislá na vnějším prostředí.

4.2.5 **Zhodnocení z hlediska finančních kritérií**

Zařízeních, které mají integrovanou webkameru lze na trhu nález mnoho. Dle cenového rádce Heuréka lze nejlevnější tablet s webkamerou koupit už za 1 190 Kč a nejlevnější notebook za 6 489 Kč, cena se ale pak i hodně odráží v kvalitě a použitelnosti zařízení. Proto je dobré držet se při výběru technických a výrobních kritérií. Trh nabízí i externí webkamery, které lze připojit k zařízení. Zde se cena pohybuje od 289 Kč do 8 790 Kč. Cena se, ale hodně odráží v kvalitě webkamery. Dražší webkamery mají větší rozlišení a větší zorný pole.

4.2.6 **Zhodnocení FRR a FAR**

Hodnota FRR u otisku prstu je často udávána 2,6 % a hodnota FAR 1,3 %
(Fujitsu Limited, 2012).
Z hodnoty FAR vidíme, že systém používající k autentizaci biometrickou metodu verifikace tváří přijme 2,6 % neoprávněných uživatelů a z hodnoty FRR vidíme, že systém neoprávněně odmítne 1,3 % uživatelů s oprávněním. Ideální zařízení nebo aplikace nevykazuje žádnou nespolehlivost nebo chybovost, když hodnota FAR a FRR se rovná nule neboli platí vztah, že **FRR=FAR=0**. (Rak, 2008)
U biometrické metody verifikace Tváří, lze pozorovat, že zařízení se stává potenciálně nebezpečné.

Ty to hodnoty jsou, ale orientační a jsou ovlivňovány nastavením vstupního citlivostního prahu.

4.3 **Verifikace hlasem**

Verifikace hlasem je jedna ještě z rozvíjejících se biometrických metod s velkým potenciálem. Jedná se o hardwarově nenáročnou biometrickou metoda. Standartním čtecím zařízením je mikrofon, který v dnešní době lze nalézt v každém mobilním zařízením.

4.3.1 **Zhodnocení z hlediska operačních kritérií**

Jedinečnost – Biometrická metoda není jedinečná pravděpodobnost schody je 1:10000.

Neměnnost – hlas se v průběhu dospívání člověka mění, a proto se nejedná neměnnou biometrickou metodu.

Měřitelnost – Biometrická metoda je měřitelná, lze jí měřit elektrostaticky.

Uchovatelnost – biometrická metoda je uchovatelná. Lze jí uchovat v podobě elektronické nahrávky stopy hlasu, která vlivem prostředí nebo časem se nezmění.

Spolehlivost – biometrická metoda je částečně spolehlivá a lze jí kdykoliv zopakovat se stejným výsledkem.

Exkluzivita – identifikační metoda je exkluzivní a není potřeba další dodatečné měřící metody.

Přijatelnost – biometrická metoda je přijatelná. Osoby neruší a nevyvolává pocity diskriminace.

Praktičnost – biometrická metoda je praktická. Osoba u ní neztratí žádný čas a nevyžaduje žádný trénink uživatele.

Uživatelská přívětivost – biometrická metoda je uživatelsky přívětivá. Osobu neruší a není vtíravá. Při snímaní osobu neruší a nediskriminuje

4.3.2 **Zhodnocení z hlediska výrobních kritérií**

Z hlediska výrobních kritérií je třeba zvážit a zaměřit se na samotnou podporu a budoucí kompatibilitu a použitý algoritmus. Samotný trh nenabízí mnoho řešení. Mnoho řešení je řešeno hlavně na zadání od odběratelů, kdy firma určí parametry a dodavatel navrhne koncepci a řešení. Tato metoda patří ještě stále do vyvíjejících se biometrických metod autentizace a do budoucna by se mohla stát velmi zajímavou alternativou otisku prstu. Z pohledu uživatele je pak důležité, aby uživatel disponoval kvalitním hardwarem.

4.3.3 **Zhodnocení z hlediska matematických, algo. a bezpečnostních kritérií**

Z hlediska matematických, algoritmických a bezpečností kritérií nelze samotnou biometrickou metodu hodnotit. Systém rozpoznání hlasu porovnává nahranou hlasovou stopu uloženou v databázi s hlasovou stopou nahranou při autentizaci, kdy podle ohodnocení schody zamezí nebo povolí přístup uživateli.

Algoritmy používané v této biometrické metodě se stále ještě vyvíjejí a vylepšují, a proto do budoucna by metoda hlas mohla být velice zajímavou bezpečnostní metodou autentizace.

4.3.4 **Zhodnocení z hlediska technických kritérií**

Z hlediska technických kritérií trh nenabízí už skoro žádné zařízení, které by nedisponovalo mikrofonem. Každý zařízení, ale má jinak výkonný mikrofon. Mikrofony mají nízkou poruchovost a nízkou náchylnost na rozbití.

4.3.5 **Zhodnocení z hlediska finančních kritérií**

Zařízeních, které mají integrovaný mikrofon lze na trhu nález mnoho. Dle cenového rádce Heuréka lze nejlevnější tablet s mikrofonem už za 1 190 Kč a nejlevnější notebook za 6 489 Kč, cena se ale pak i hodně odráží v kvalitě použitého mikrofonu v zařízení. Proto je dobré držet se při výběru technických a výrobních kritérií. Trh nabízí i externí mikrofony, které lze připojit k zařízení. Zde se cena pohybuje od 39 Kč do 7 790 Kč. Cena se, ale hodně odráží v kvalitě. Dražší mikrofony mají větší frekvenční rozsah, větší SPL(Sound Pressure Leve), citlivost a lepší odstup signálu.

4.3.6 **Zhodnocení FRR a FAR**

Hodnota FRR u biometrické metody verifikace hlasem je často udávána 0,3 % a hodnota FAR 0.01% (Fujitsu Limited, 2012).

Z hodnoty FAR vidíme, že systém používající k autentizaci biometrickou metodu verifikace hlasem přijme 0,01 % neoprávněných uživatelů a z hodnoty FRR vidíme, že systém neoprávněně odmítne 0,3 % uživatelů s oprávněním. Ideální zařízení nebo aplikace nevykazuje žádnou nespolehlivost nebo chybovost, když hodnota FAR a FRR se rovná nule neboli platí vztah, že **FRR=FAR=0**. (Rak, 2008)Biometrická metoda verifikace hlasem, je spolehlivější než metoda biometrická metoda verifikace obličejem, ale její hodnoty FAR a FRR se nerovnají nule a jsou horší než hodnoty u biometrické metody otisk prstu.

Ty to hodnoty jsou, ale orientační a jsou ovlivňovány nastavením vstupního citlivostního prahu.

4.4 Vyhodnocení biometrických metod otisk prstu, tvář a hlas

Shrnutí operační Kritéria

Ze zhodnocení operačními kritérii vychází otisk prstu jako nejlepší biometrická metoda (viz Tabulka 6), a to kvůli kritériím neměnnost, jedinečnost, měřitelnost. Otisk prstu je jediná ze tří biometrických metod, která po celý život zůstává stejná a nemění se, na rozdíl od biometrických metod tvář a hlas, které se po celí život člověka mění. Z hlediska kritéria spolehlivost, je shoda u otisku prstu 1:1000000 u hlasu 1:10000 a tváře není hodnota dána, kvůli výskytu jednovaječných dvojčat, kde byli naměřeny schody 1:1. Zbylá kritéria splňují všechny tři biometrické metody.

Tabulka 6 Operační kritéria zhodnocení

OPERAČNÍ KRITÉRIA			
KRITÉRIUM	**OTISK PRSTU**	**TVÁŘ**	**HLAS**
Jedinečnost	*NE*	*NE*	*NE*
Neměnnost	*ANO*	*NE*	*NE*
Měřitelnost	*ANO*	*ANO*	*ANO*
Uchovatelnost	*ANO*	*ANO*	*ANO*
Spolehlivost	*ANO*	*ANO*	*ANO*
Exkluzivita	*ANO*	*ANO*	*ANO*
Přijatelnost	*ANO*	*ANO*	*ANO*
Praktičnost	*ANO*	*ANO*	*ANO*
Uživatelská přívětivost	*ANO*	*ANO*	*ANO*

Zdroj: (vlastní práce, 2020)

Shrnutí výrobní kritéria

Z hlediska výrobních kritérií otisk prstu kvůli své vysoké dostupnosti ve všech zařízeních a mnoha řešením na trhu, vychází jako nejvíc přijatelná biometrická metoda jak z pohledu uživatele v rámci dostupnosti, tak i z pohledu banky, kvůli mnoha řešením, který trh nabízí. Biometrickou metodu otisk prstu bych doporučil i z hlediska podpory nebo kompatibility, kvůli rozšířenosti a rozsahu používání.

Ty to dva ukazatele nám můžou naznačit, že tato metoda bude ještě dlouhou dobu podporovaná a kompatibilní s jinými systémy.

Shrnutí matematický, algoritmický. a bezpečnostních kritéria

Z hlediska Matematických, algoritmických a bezpečnostních kritérií vychází nejlépe metoda otisk prstu. Každé zařízení s čtečkou otisku prstu má v sobě už implementovaný algoritmy. Každý algoritmus je výrobcem odzkoušený a má svůj certifikát. Zařízení disponující s mikrofonem nebo webkamerou nemají v mnoha případech v sobě žádný algoritmy.

Shrnutí technický kritéria

Z hlediska technických kritérií vychází nejlépe biometrická metoda hlas, kvůli dostupnosti mikrofonu u dvou zařízení již v základu, nízké poruchovosti mikrofonů a nízké náchylnosti k rozbití.

Shrnutí finanční kritéria

Z hlediska finančních kritérií vychází nejlépe biometrická metoda hlas (viz Tabulka 7). Kvůli cenově nejdostupnějším zařízením. Dle cenového rádce Heureka, lze sehnat tablet s mikrofonem už od 1 190 Kč, notebook od 6 489 Kč a mikrofon se stolním počítačem a příslušenstvím od 8 808 Kč pří ceně stolního počítače a příslušenství 8 769 Kč. Druhým nejdostupnějším je biometrické metoda tvář s tabletem, který lze sehnat od 1 190 Kč, notebookem od 6 489 Kč a webkameru se stolním počítačem a příslušenstvím od 9 085 Kč pří ceně stolního počítače a příslušenství 8 769 Kč.

Nejdražší biometrickou metou je otisk prstu. Tablet s čtečkou otisku prstu lze koupit od 8 893 Kč, notebook od 6 489 Kč a externí čtečku otisků prstů se stolním počítačem a příslušenstvím od 9 976 Kč pří ceně stolního počítače a příslušenství 8 769 Kč.

Tabulka 7 Finanční kritéria zhodnocení

FINANČNÍ KRITÉRIA			
ZAŘÍZENÍ	**OTISK PRSTU**	**TVÁŘ**	**HLAS**
Notebook	*6 489 Kč*	*6 489 Kč*	*6 489 Kč*
Tablet	*8 893 Kč*	*1 190 Kč*	*1 190 Kč*
Stolní počítač	*9 976 Kč*	*9 058 Kč*	*8 808 Kč*

Zdroj: (vlastní práce, 2020)

Shrnutí FRR a FAR kritéria

Z hlediska kritérií FRR a FAR vychází nejlépe biometrická metoda otisk prstu (viz Tabulka 8). Hodnoty FRR a FAR se u biometrické metody otisk prstu blíží ke vztahu, že FRR = FAR = 0. Alternativou pro biometrickou metodu otisk prstu je biometrická metoda Hlas s hodnotami FRR 0,3 % a FAR 0,01 %. Za nejhorší biometrickou metodu z pohledu kritérií FRR A FAR lze označit biometrickou metodu tvář.

Tabulka 8 FRR a FAR kritéria zhodnocení

FRR A FAR KRITÉRIA		
BIOMETRICKÁ METODA	**FRR %**	**FAR %**
Otisk prstu	0,1	0,001
Tvář	2,6	0,3
Hlas	0,3	0,01

Zdroj: (vlastní práce, 2020)

4.5 Návrh koncepce zabezpečení autentizace s využitím biometrické metody

Na základě informací a analýz získaných z předchozích kapitol, je sestaven následujíc model třífázové autentizace s využitím biometrické metody otisk prstu k lepšímu zabezpečení, který by umožnilo od opuštění autorizace požadavků v internetovém bankovnictví a uživateli by ušetřila čas a zjednodušila práci. Dále by uživateli umožňovala založení a vyřízení hypotéky nebo půjčky v internetovém bankovnictví bez nutnosti zajít na pobočku banky.

Při konstrukci fází ověřování byl kladen velký důraz na bezpečnost, efektivnost a budoucí využitelnost bez nutnosti měnit parametry.

Návrh tří fázové autentizace pro internetové bankovnictví se bude skládat ze tří fází (znalostní, vlastnická, biometrická), kdy každá fáze bude popsána. Poslední fáze autentizace se bude zakládat na použití biometrické metody. Nejlépe vyhodnocená biometrická metoda bude doporučená v závěru bakalářské práce.

4.5.1 **První Fáze**

První fáze autentizace (viz Obrázek 5), kterou můžeme nazvat „fází znalostní“, se bude skládat z identifikačního čísla a hesla. Identifikační číslo bude uživateli vygenerované a přidělené. Pro první přihlášení bude uživateli heslo vygenerované a spolu s identifikačním číslem odeslané na e-mailovou adresu zadanou uživatelem při zakládání účtu.

V první fázi uživatel zadá své identifikační číslo a heslo. Odpovědí systému na požadavek uživatele je posun do druhé fáze autentizace, za předpokladu, že uživatel zadal správně uživatelské heslo a identifikační číslo. Při špatném zadání uživatelského hesla nebo identifikačního čísla je uživatel upozorněný hláškou “invalid password or identification number“ (neplatné heslo nebo identifikační číslo) a není posunut do druhé fáze autentizace.

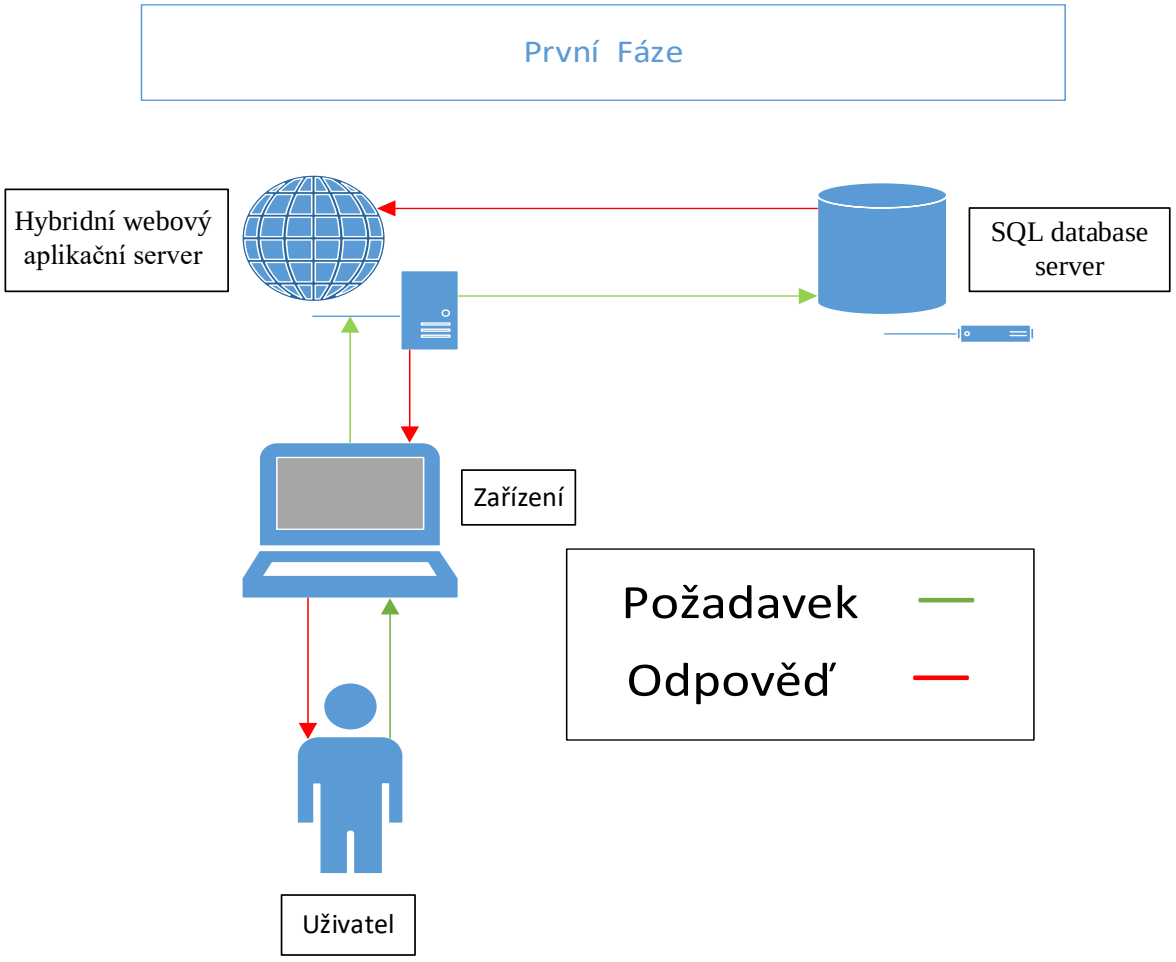
Průběh první fáze autentizace:

1) Uživatel zadá uživatelské identifikační číslo a heslo
2) Počítač/notebook/tablet odešle požadavek ověření na hybridní webový aplikační server
3) Server po obdržení požadavku od počítače/notebooku/tabletu pošle požadavek na SQL database server kde se zadané heslo porovná s heslem v SQL database serveru podle ID co uživatel zadal a které slouží jako identifikátor uživatele
4) SQL database server pošle odpověď hybridnímu webovému aplikačnímu serveru
5) Hybridní aplikační server pošle odpověď na počítač/notebook/tablet
6) Počítač/notebook/tablet zobrazí odpověď uživateli

6.1) invalid password or identification (neplatné heslo nebo identifikační číslo) a znemožní přístup uživateli do internetového bankovnictví. Uživatel je nucen opakovat celý proces autentizace od první fáze

6.2) valid password or identification (platné heslo nebo identifikační číslo) a posune uživatele do druhé fáze autentizace

Obrázek 5 První fáze autentizace



Zdroj: (vlastní práce, 2020)

Délka identifikačního čísla je zvolená tak aby byl dostatek číselných variací, který by pokryli celou populaci planety země a vystačili dále než do roku 2056, kdy dle nasimulovaných statistických údajů by populace planety země měla být 10 miliard lidí. Data vývoje populace jsou jen orientační a vychází z dat získaných na internetové stránce (Population.City, 2015).

Výpočet:

Světová populace v roce 2056: 10 miliard

Současná světová populace: 7,7 miliard

V´=100 000 000 000 – počet variací (vychází z podmínek)

V´>7 700 000 000 – podmínka představující kdy počet variací musí být větší než 7,7 Miliard

V´>10 000 000 000 – podmínka představující kdy počet variací musí být větší než 10 Miliard

k:? – délka čísla

n:10 – počet znaků ze kterých se může číslo skládat (0,1,2,3,4,5,6,7,8,9)

Vycházíme ze vzorce pro variace s opakováním (kombinatorika):

Rovnice 5 Variace s opakováním

$$V´(k,n) = n^k$$

Po dosazení do vzorce a úpravách nám vyjde, že je potřeba jedenáctimístné číslo, aby pokrylo celou populaci až do roku 2056.

$$\begin{aligned} 100000000000 &= 10^k \\ 10^{11} &= 10^k \\ 11 &= k \end{aligned}$$

Identifikační číslo se z hlediska budoucího celosvětového využití skládá z jedenáctimístného čísla a je složeno z číslic 0,1,2,3,4,5,6,7,8,9 s podmínkou, že čísla se můžou opakovat.

Délka a bezpečnost hesla je určená tak, že vycházím z doporučení od (Bitto, 2005a) a dále jsem je upravil dle zkušeností nasbíraných na pozici IT Support Specialista ve firmě Sotio a.s, tak aby odolala slovníkovému útoku a jeho variacím jako například slovníkový útok s přidanými permutacemi nebo jiným útokům jako jsou například PA(Passwords Attack), PCA(Password Cache Attack), PBFA(Preliminary Brute Force Attack), FPA (Found Passwords Attack).

Parametry hesla:

- Délka minimálně 12 znaků
- Obsahuje velká a malá písmena standartní anglické abecedy
- Obsahuje číslice
- Obsahuje speciální znaky (například:?, !, @, %, $, &,* ,+ ,-, =.. a další)

Při nastavených hodnotách, ale není zaručena 100% bezpečnost hesla. Bezpečnost hesla ovlivňuje hodně i sám uživatel.
Například mnoha uživatelů používá stejné heslo ke všem s vím přístupům. Při prolomení jedno přístupu se heslo stává nebezpečným a útočník ho zapíše do slovníku, který pak útočník nebo útočníci (jedná-li se o sdílený slovník) používá při útoku FPA nebo PCA.

4.5.2 **Druhá Fáze**

Druhá fáze autentizace (viz Obrázek 6), kterou můžeme nazvat fází „vlastnickou“ se zakládá na metodě autentizace za pomoci SMS kódu nebo Tokenu. Uživatel má možnost výběru, jakou metodou se v dané chvíli chce autentizovat kvůli zaručení možnosti přihlášení, kdyby jedna z metod nebyla dostupná. Přiklad: uživatel používá metodu Tokenu, který je součástí mobilní aplikace, ale zapomněl, jaký heslo má nastavené v aplikaci nebo aplikace je nefunkční po posledním updatu.

Obě metody autentizace byli vybrány na základě jejich bezpečnosti a rešerši metod autentizací které nabízí pět největších bank v české republice v teoretické části bakalářské práce.

V druhé fázi autentizace je uživatel vyzván, aby prokázal svou identitu vlastnictvím Tokenu. Vlastnictví tokenu uživatel prokáže přihlášením do mobilní aplikace a potvrzením požadavku o přihlášení do internetového bankovnictví. Na prokázání vlastnictví tokenu

běží uživateli časový limit pět minut. Při neprokázání do časového limitu systém zamezí přístup do internetového bankovnictví a uživatel se musí znovu autentizovat do internetového bankovnictví od první fáze.

Uživateli je taky nabídnuta možnost, zda se nechce autentizovat za pomoci SMS kódu. Při volbě autentizace SMS kódem, je uživateli systémem zaslán šesti místní kód na telefonní číslo, které zadal při zakládání bankovního účtu. Uživatel má při této metodě autentizace tři pokusy na správné zadání kódu. Když uživatel zadá kód třikrát špatně, systém zamezí přístup do internetového bankovnictví a uživatel se musí znovu autentizovat do internetového bankovnictví od první fáze.

Při prokázání vlastnictví metodou autentizace SMS kód nebo Token. Systém odpoví posunem uživatele do třetí fáze autentizace.

Průběh druhé fáze autentizace:

1) Hybridní webový aplikační server (dále už jen server) pošle odpověď na počítač/notebook/tablet a požadavek do aplikace mobilní bankovnictví na telefonu uživatele
2) Počítač/notebook/tablet zobrazí odpověď uživateli: Please confirm the request for motion banking or select the SMS code identification method (Prosím o potvrzení požadavku ve vašem mobilním bankovnictví nebo zvolte metodu identifikace SMS kód) a běží časová lhůta 5 min na potvrzení požadavku v mobilním bankovnictví nebo zvolení metody identifikace SMS kód
3) Potvrzení za pomoci Tokenu nebo SMS kódu
   3.1) Potvrzení za pomoci Tokenu
      3.1.1) Uživatel se přihlásí do mobilní aplikace a potvrdí požadavek
      3.1.2) Mobilní aplikace pošle odpověď na server
      3.1.3) Server pošle odpověď na počítač/notebook/tablet
      3.1.4) Počítač/notebook/tablet zobrazí odpověď uživateli
         3.1.4.1) Confirmed (Potvrzeno) a posune uživatele do třetí fáze autentizace

3.1.4.2) Timed out (Čas vypršel) a systém zamezí přístup do internetového bankovnictví a uživatel se musí znovu autentizovat do internetového bankovnictví od první fáze

3.2) Potvrzení za pomoci SMS kódu

3.2.1) Uživatel zvolil potvrzení za pomoci SMS kódu

3.2.2) Počítač/notebook/tablet pošle požadavek na server

3.2.3) Server pošle odpověď: šestimístný kód na telefonní číslo co uživatel zadal při zakládání bankovního účtu

3.2.4) Uživatel zadá šestimístný kód do počítače/notebooku/tabletu

3.2.5) Počítač/notebook/tablet pošle požadavek na server

3.2.6) Server pošle odpověď na počítač/notebook/tablet

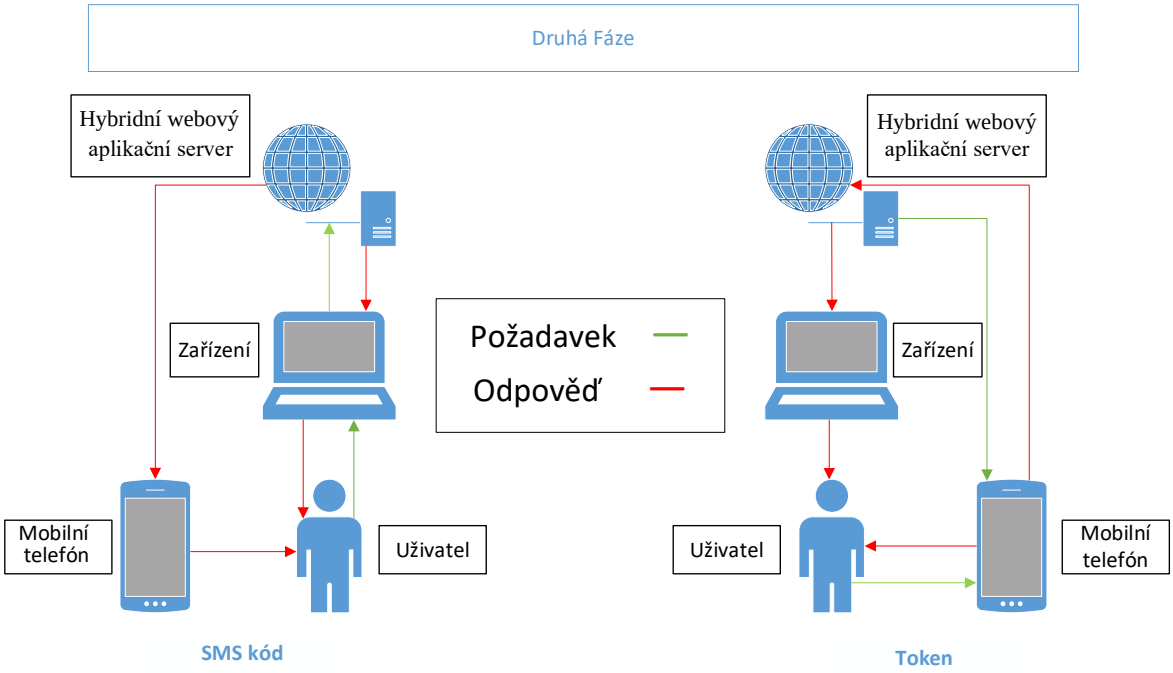
3.2.7) Počítač/notebook/tablet zobrazí odpověď uživateli

3.2.7.1) Valid code (Platný kód) a posune uživatele do třetí fáze autentizace

3.2.7.2) Invalid code (Neplatný kód) a vyzve uživatele, aby kód zadal znovu

3.2.7.3) 3x invalid code (3x neplatný kód) a znemožní přístup uživateli do internetového bankovnictví. Uživatel je nucen opakovat celý proces autentizace od první fáze

Obrázek 6 Druhá fáze autentizace



Hybridní webový aplikační server

Zdroj: (vlastní práce, 2020)

Kvůli bezpečnosti a pokrytí všech lidí se SMS kód skládá z šesti čísel, které jsou tvořeny velkými nebo malými písmeny anglické abecedy a čísly, který se mohou opakovat.

Pro určení velkosti kódu byli použity ty to podmínky:

Světová populace v roce 2056 dle (Population.City, 2015): 10 miliard
Současná světová populace dle (Population.City, 2015): 7,7 miliard
Výkon počítačové jednotky dle (RADEK BENEŠ, 2013): 10 miliónů porovnání a vyhodnocení za sekundu

Při použití vzorce pro variaci, s opakování zjistíme, že kód o velikosti 6 míst s 62 možnostmi znaků má 56 800 235 584 variací. S podmínkou tří pokusů na správné zadání se jedná o silný bezpečnostní kód, který pokryje všechny lidi při autentizaci za pomoci SMS kódu.

Výpočet:

k:6 – délka kódu

n: – počet znaků ze kterých se může kód skládat

(0,1,2,3,4,5,6,7,8,9,A,a,B,b,C,c,D,d,E,e,F,f,G,g,H,h,I,i,J,j,K,k,L,l,M,m,N,n,O,o,P,p,Q,q,R,r,S,s,T,t,U,u,V,v,W,w,X,x,Y,y,Z,z)

Rovnice 6 Variace s opakováním

$$V'(k,n) = n^k$$

$$V' = 62^6$$

$$V' = 56\,800\,235\,584$$

4.5.3 **Třetí Fáze**

Třetí fáze autentizace (viz Obrázek 7), kterou můžeme nazvat fází biometrickou se zakládá na autentizaci biometrickou metodou otisk prstu. Při této fázi je uživatel vyzván systémem, aby svoji identitu doložil biometrickým parametrem otisk prstu. Na doložení biometrického parametru má tři pokusy, kdyby při snímaní došlo k chybě nebo biometrický parametr byl nasnímán špatně. Systém tu to skutečnost oznámí hláškou “Badly entered biometric parameter finger print“ („špatně zadaný biometrický parametr otisk prstu“).

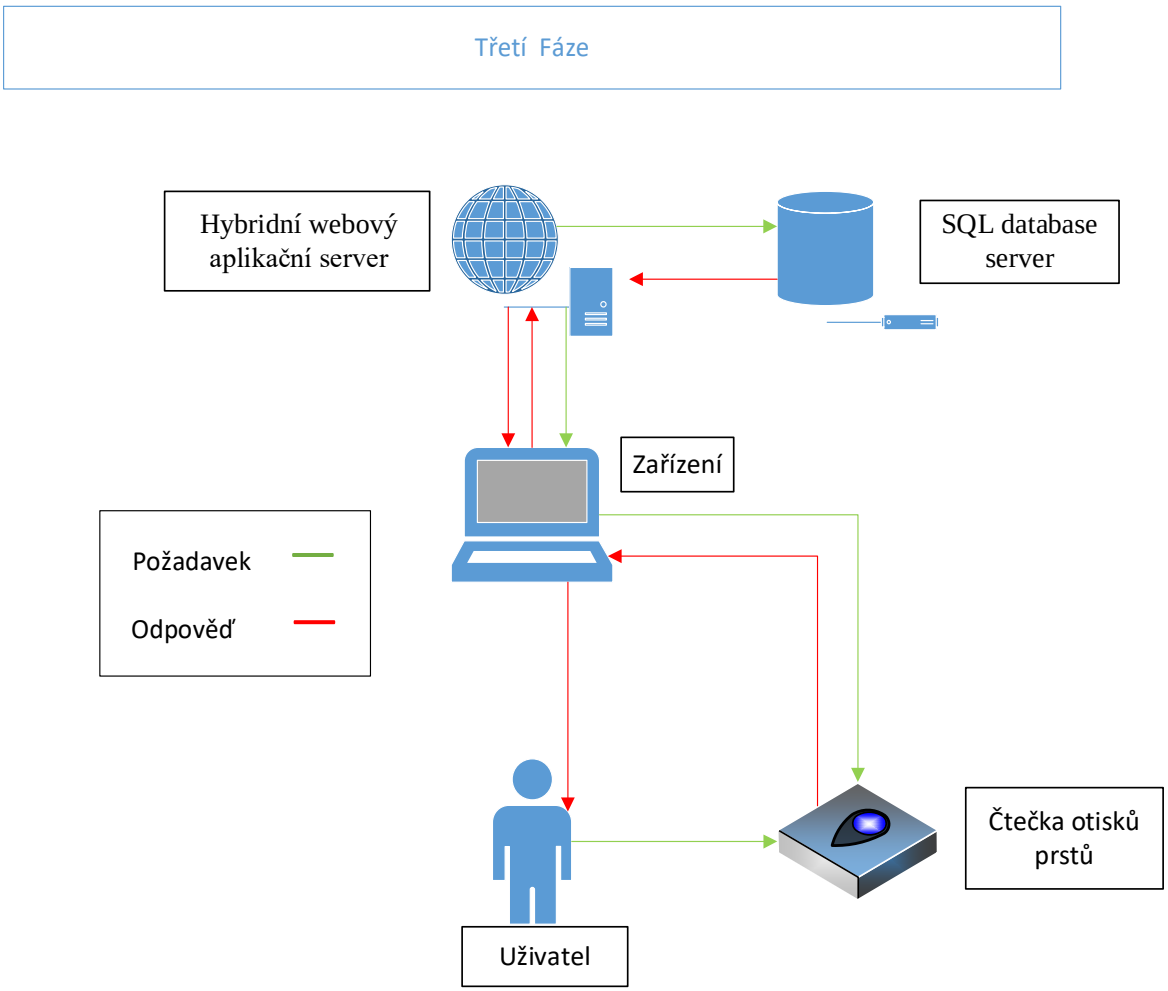
Při špatném zadání biometrického parametru třikrát, systém zamezí přístup do internetového bankovnictví a uživatel je nucen začít s autentizací znovu od začátku.

Při platným zadání biometrického parametru, systém ověří v databázi, zda se jedná o platný biometrický parametr. Při platném biometrickém parametru je uživateli umožněn přístup a práce v internetovém bankovnictví a uživateli se zobrazí pracovní rozhraní internetového bankovnictví. Při neplatným biometrickým parametru systém zobrazí chybovou hlášku “Invalid biometric parameter finger print“ („neplatný biometrický parametr otisk prstu“) a znemožní přístup uživateli do internetového bankovnictví. Uživatel je nucen opakovat celý proces autentizace od první fáze.

Průběh třetí fáze autentizace:

1) Hybridní webový aplikační server (dále už jen Server) pošle požadavek na počítač/notebook/tablet
2) Počítač/notebook/tablet pošle požadavek na čtecí biometrické zařízení a pošle odpověď uživateli
3) Uživatele se prokáže biometrickým parametrem otisk prstu na čtecím biometrickém zařízení
   3.1) Při špatném nasnímaní biometrického parametru nebo chybě při snímání počítač/notebook/tablet zobrazí hlášku Badly entered biometric parameter finger print (Špatně zadaný biometrický parametr otisk prstu)
   3.2) Při třetím špatném nasnímaní biometrického parametru nebo chybě při snímán počítač/notebook/tablet zobrazí hlášku Invalid attempt to log in to internet banking (Neplatný pokus o přihlášení do internetového bankovnictví) a znemožní přístup uživateli do internetového bankovnictví. Uživatel je nucen opakovat celý proces autentizace od první fáze
   3.3) Při platným zadání biometrického parametru, čtecí biometrické zařízení pošle odpověď počítači/notebooku/tabletu
4) Počítač/notebook/tablet pošle odpověď hybridnímu aplikačnímu serveru
5) Server pošle požadavek na porovnání biometrického parametru s biometrickým parametrem uloženým na SQL database server
6) SQL database server pošle odpověď na server
7) Server pošle odpověď na počítač/notebook/tablet
8) Počítač/notebook/tablet zobrazí odpověď uživateli
   8.1) Invalid biometric parameter finger print (Neplatný biometrický parametr otisk prstu) a znemožní přístup uživateli do internetového bankovnictví. Uživatel je nucen opakovat celý proces autentizace od první fáze
   8.2) Valid biometric parameter finger print (Platný biometrický parametr otisk prstu) a je uživateli umožněn přístup a práce v internetovém bankovnictví a zobrazí se pracovní rozhraní internetového bankovnictví

Obrázek 7 Třetí fáze autentizace



Zdroj: (vlastní práce, 2020)

5 Výsledky a diskuse

V této části bakalářské práce shrnu výsledky biometrických metod otisk prstu, tvář, hlas a shrnu model třífázové autentizace s využitím biometrické metody otisk prstu a jeho budoucí potenciál, který nabízí.

5.1 Verifikace biometrickou metodou Otisk prstu

Biometrická metoda otisk prstu je ze všech nejrozšířenější bezpečnostní metodou verifikace po celém světě. Čtečku otisku prstu lze nalézt díky své malé velikosti a druhům technologií čteček v téhle době na každém zařízení.
Čtečkou otisku prstu disponuje notebook, tablet, ale i stolní počítač po připojení externí čtečky. Biometrická metoda otisku prstu je velice přesná biometrická metoda, která je po celý život stálá a časem neměnná. Biometrická metoda je analogově, tak digitálně dobře uchovatelná. Biometrická metoda otisk prstu má, ale i své nevýhody. Jedna z nevýhod je lehkost zanechání otisku prstu na každém předmětu a jednoduchá výroba falsifikátu. V dnešní době už, ale existují čtečky otisků prstů, kterou jsou založené na technologii, která rozezná, že se jedná o falsifikát.

Z pohledu FAR a FFR se nejedná o biometrickou metodu, která by nevykazovalo chyby a byla stoprocentně spolehlivé. Hodnoty FAR a FRR jsou ale lepší než u biometrický metody využívající hlas nebo tvář uživatele.

Výhody:

- přesnost
- částečná spolehlivost
- stálost
- velikost snímače
- uchovatelnost

Nevýhody:

- náchylnost na útoky
- jednoduché zanechání otisku na věcech, které může vést k zneužití

5.2 Verifikace biometrickou metodou Tvář

Biometrická metoda Tvář je druhá nejpoužívanější bezpečnostní metoda na světě. Lze jí nalézt na mobilních telefonech, počítačích ale i na letišti sloužící k identifikaci osob. Existuje mnoho algoritmů identifikace tváře uživatele, ale žádný algoritmus není dokonalý. To naznačuje i vysoký číslo FAR a FRR, ale z pohledu uživatele se jedná o nejvíce přívětivou biometrickou metodu.
Verifikaci tváří je vysoce ovlivněná použitým hardwarem a prostředím kde se uživatel nachází.
V prašnému prostředí nebo prostředí s nízkou nebo vysokou teplotou a vysokou vlhkostí se biometrická metoda stává nepoužitelnou.
Při nedostatečném rozlišení kamery se prodlužuje rychlost verifikace a výkonnost systému.

Výhody:

- uživatelská přívětivost

Nevýhody:

- nepříliš přesná metoda
- měnnost obličeje časem
- nejednoznačnost

5.3 Verifikace biometrickou metodou Hlas

Biometrická metoda hlas je stále rozvíjející a zkoumaná biometrická metoda.
Jedná se o uživatelsky nejpřívětivější biometrickou metodu, která je ale vysoce ovlivněná parametry použitého hardwaru, stavu uživatele a prostředí.

Z pohledu FAR a FFR se nejedná o biometrickou metodu, která by nevykazovalo chyby a byla stoprocentně spolehlivé.
Hodnoty FAR a FRR jsou ale lepší než u biometrický metody využívající tvář uživatele a horší, než u biometrické metody využívají otisk prstu.

Výhody:

- částečná spolehlivost.

Nevýhody:

- při únavě, stresu nebo nemoci uživatele systém nemusí správně identifikovat
- špatná identifikace v rušné prostředí

5.4 Model třífázové autentizace s využitím biometrické metody otisk prstu

Model třífázové autentizace využívající biometrickou metodu otisk prstu je založen na třífázové autentizaci. První fáze autentizace se skládá z jedenáctimístného identifikačního čísla a nejméně dvanáctimístného hesla. Identifikační číslo bylo vytvořeno tak aby pokrylo celou planetu zemi v přítomnosti, ale i v budoucnosti a v případě i když by internetovým bankovnictvím disponovali všichni lidi na světě. Druhá fáze autentizace se skládá z SMS klíče nebo Tokenu, kdy uživatel má možnost volby dle dostupnosti a jeho preferencí. Třetí fáze autentizace se skládá z biometrické metody otisk prstu. Při splnění všech tří autentizačních kroků je uživateli povolen přístup do internetového bankovnictví. Model třífázové autentizace byl navržen pro zlepšení bezpečnosti přihlašování uživatele do internetového bankovnictví, které by bankám do budoucnosti umožnilo aplikovat veškeré služby do internetového bankovnictví a použít biometrickou metodu otisk prstu jako elektronický podpis. Výhodou tohoto řešení je zlepšení bezpečnosti autentizace do internetového bankovnictví, možné snížení nákladů banky na pobočky, možné zamezení ztráty času uživatele, který by strávil v pobočce při vyřizování, možné snížení lidské stopy na planetě zemi v podobě snížení papírování a převedení všech dokumentů do elektronické verze s možností elektronického podpisu s nejvyšší autoritou.

6 Závěr

Cílem bakalářské práce bylo zhodnotit metody biometrického zabezpečení vhodné pro posílení autentizace klienta do internetového bankovnictví a navrhnout třífázovou autentizaci klienta do internetového bankovnictví s biometrickou metodou.

V teoretické části bakalářské práce byl vymezen pojem internetové bankovnictví a byli zhodnoceny metody autentizace do internetového bankovnictví a analyzována nabídka metod autentizace bank v české republice. Konkrétně byli hodnoceni ty to banky České spořitelna, ČSOB, Komerční Banka, Moneta Money Bank, Fio Banka, které byli vybrány podle počtu klientů v české republice.

Dále byl vymezen pojem biometrie a analyzovány biometrické metody otisk prstu, tvář a hlas. Následně byli analyzovány možnosti hodnocení biometrických metod kritérii pro biometrické metody a kritérii pro měření výkonosti biometrických metod.

V praktické části bakalářské práce byly provedeny zhodnocení vybraných biometrických metod otisk prstu, hlas a tvář. V dalším kroku byl navržen návrh tří fázové autentizace do internetového bankovnictví, která využívá jako jednu z fází ověření na základě biometrického údaje otisk prstu. Biometrická metoda byla vybrána na základě výsledků z hodnocení biometrických metod kritérii pro biometrické metody a kritérii pro měření výkonosti biometrických metod, kde biometrická metoda otisk prstu byla dle FRR a FAR, operačních kritérií, pravděpodobnosti chybného přijetí a odmítnutí, technických kritérií a matematických, algoritmických a bezpečnostních kritérií zhodnocená jako nejlépe možnou biometrickou metodou k nasazení do tří fázové autentizace do internetového bankovnictví.

V závěru bakalářské práce byli zhodnoceny biometrické metody autentizace otisk prstu, tvář, hlas a na základě zhodnocení byla vybrána biometrická metoda otisk prstu a doporučená k nasazení do návrhu tří fázové autentizace klienta do internetového bankovnictví. Následně se zhodnotili a analyzovali možnosti navrženého modelu třífázové autentizace.

7 Seznam použitých zdrojů

BEŇOVIČ, Aleš, 2020. EXTERNÍ ČTEČKA OTISKŮ PRSTŮ. In: *Www.svetalarmu.cz* [online]. Ostrava: Aleš Beňovič [cit. 2020-09-06]. Dostupné z: https://www.svetalarmu.cz/pristupove-systemy/9137423e-externi-ctecka-otisku-prstu-usb-438.html?SubmitCurrency=1&id_currency=1

Biometrie otisku prstu, c2011-2020. *Biometric Line* [online]. Brno: ABBAS, a.s. [cit. 2020-09-21]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

BITTO, Ondřej, 2005a. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 94. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005b. BITTO, Ondřej. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 93-94. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005c. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 118. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005d. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 118. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005e. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 140. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005f. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 124. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005g. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 139. ISBN 80-86686-48-5.

BITTO, Ondřej, 2005h. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, s. 122. ISBN 80-86686-48-5.

BUREŠ, Michal, 2020. Kam plyne zisk 78 miliard Kč z českých bank?. *Finance.cz* [online]. Praha: Mladá fronta a.s. [cit. 2020-09-06]. Dostupné z: https://www.finance.cz/496071-kdo-vlastni-ceske-banky/

ČERNOHORSKÝ, Jiří, 2003. Biometrie. *Časopis Automa* [online]. Děčín: Automa – časopis pro automatizační techniku, s. r. o. [cit. 2020-09-06]. Dostupné z: https://automa.cz/cz/casopis-clanky/biometrie-2003_07_28872_02022/

ČESKÁ SPOŘITELNA, 2020. Bankovní IDentita. *Česká spořitelna* [online]. Praha: Česká spořitelna [cit. 2020-09-06]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita

Česká spořitelna Všeobecná prezentace o Finanční skupině ČS, 2020. *Česká spořitelna* [online]. Praha: Česká spořitelna [cit. 2020-09-06]. Dostupné z: https://www.csas.cz/static_internet/cs/Obecne_informace/FSCS/CS/Prilohy/vseobecna_prezentace.pdf

CIESLAR, Jan, 2019. Internetové bankovnictví využívá 5,5 milionu Čechů. *Český statistický úřád* [online]. Praha: ČSÚ [cit. 2020-09-06]. Dostupné z: https://www.czso.cz/csu/czso/internetove-bankovnictvi-vyuziva-55-milionu-cechu

ČSOB, 2018. S internetem šetřím svůj čas a peníze ČSOB: InternetBanking 24. *ČSOB* [online]. Praha: Československá obchodní banka, a. s. [cit. 2020-09-06]. Dostupné z: https://www.csob.cz/portal/documents/10710/36574/csob-ib24-prirucka-zkrac.pdf

Čtečky otisků prstů v mobilech: typy a funkce, 2020. *Alza.cz* [online]. Praha: Alza.cz a.s. [cit. 2020-09-21]. Dostupné z: https://www.alza.cz/ctecka-otisku-prstu-typy-funkce#typy

Fakta a výsledky, 2020. *Komerční banka* [online]. Praha: Komerční banka [cit. 2020-09-06]. Dostupné z: https://www.kb.cz/cs/o-bance/vse-o-kb/fakta-a-vysledky

FIO BANKA, 2020. Zabezpečení. *Fio banka* [online]. Praha: Fio banka, a.s. [cit. 2020-09-06]. Dostupné z: https://www.fio.cz/bankovni-sluzby/internetbanking/zabezpeceni

FUJITSU LIMITED, 2012. PalmSecure – Biometric Technology Vaše ruka je klíčem. *Isss* [online]. Tokio: Fujitsu Limited [cit. 2020-09-06]. Dostupné z: https://www.isss.cz/archiv/2014/download/prezentace/fujitsu_podivin.pdf

Historie KB, 2020. *Komerční banka* [online]. Praha: Komerční banka [cit. 2020-09-06]. Dostupné z: https://www.kb.cz/cs/o-bance/vse-o-kb/kb-historie

Historie MONETA Money Bank, 2020. *MONETA Money Bank* [online]. Praha: MONETA Money Bank, a. s. [cit. 2020-09-06]. Dostupné z: https://www.moneta.cz/o-nas/historie

Historie, 2020. *Fio banka* [online]. Praha: Fio banka, a.s. [cit. 2020-09-06]. Dostupné z: https://www.fio.cz/o-nas/fio-banka/historie

HNÍK, Václav, Oldřich KRULÍK a Eva STAŇOVÁ, 2020. Základy bezpečnosti na Internetu. In: *Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra české republiky [cit. 2020-09-28]. Dostupné z: https://www.mvcr.cz/soubor/cyber-vyzkum-studie-rady-pdf.aspx.

HOVORKA, Jiří, 2020. Největší banky v Česku. Žebříček podle počtu klientů i peněz. *Peníze.cz* [online]. Praha: Peníze.cz [cit. 2020-09-06]. Dostupné z: https://www.penize.cz/bezne-ucty/413386-nejvetsi-banky-v-cesku-zebricek-podle-poctu-klientu-i-penez

Internetové bankovnictví, c2011-2020. *Equa bank* [online]. Praha: Equa Bank [cit. 2020-09-06]. Dostupné z: https://www.equabank.cz/bezny-ucet/internetove-bankovnictvi

KB, 2020. *Nové způsoby přihlášení* [online]. Praha: Komerční banka [cit. 2020-09-06]. Dostupné z: https://www.kb.cz/cs/nove-zpusoby-prihlaseni#jaknato

Kdo jsme, 2020. *Česká spořitelna* [online]. Praha: Česká spořitelna [cit. 2020-09-06]. Dostupné z: https://www.csas.cz/cs/o-nas/kdo-jsme

KOVANDA, Radek, 2018. 3 typy otisků, tři typy lidí: který z nich jste vy?. In: *G.cz* [online]. Praha: Extra Online Media s.r.o. [cit. 2020-09-06]. Dostupné z: https://g.cz/3-typy-otisku-tri-typy-lidi-ktery-z-nich-jste-vy/

LUDVÍK, Miroslav, 2004. Autentizační prvky a metody pod drobnohledem II. *Peníze.cz* [online]. Praha: Peníze.cz [cit. 2020-09-06]. Dostupné z: https://www.penize.cz/investice/16780-autentizacni-prvky-a-metody-pod-drobnohledem-ii

MATYÁŠ, Vašek a Jan KRHOVJÁK, 2008c. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. 1. vyd. Brno: Masarykova univerzita. ISBN 978-80-210-4556-9.

MATYÁŠ, Vašek, Jan KRHOVJÁK, Marek KUMPOŠT a Václav LORENC, 2008a.

Principy slabé a silné autentizace uživatelů. VAŠEK, Matyáš, Jan KRHOVJÁK, Marek KUMPOŠT a Václav LORENC. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. 1. vyd. Brno: Masarykova univerzita, s. 25. ISBN 978-80-210-4556-9.

MATYÁŠ, Vašek, Jan KRHOVJÁK, Václav LORENC a Marek KUMPOŠT, 2008b.

MATYÁŠ, Vašek, Jan KRHOVJÁK, Václav LORENC a Marek KUMPOŠT. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, s. 80-82. ISBN 978-80-210-4556-9.

MIROSLAV, Ludvík, 2004. Autentizační prvky a metody pod drobnohledem. *Peníze.cz* [online]. Praha: Partners media, s.r.o. [cit. 2020-09-06]. Dostupné z: https://www.penize.cz/investice/16777-autentizacni-prvky-a-metody-pod-drobnohledem

MONETA MONEY BANK, 2020. Internet Banka MONETA Money Bank. *MONETA: money bank* [online]. Praha: MONETA Money Bank, a. s. [cit. 2020-09-06]. Dostupné z: https://www.moneta.cz/lide/prime-bankovnictvi/internet-banka

O ČSOB a skupině, 2020. *ČSOB* [online]. Praha: Československá obchodní banka, a. s. [cit. 2020-09-06]. Dostupné z: https://www.csob.cz/portal/csob/o-csob-a-skupine

Otisk prstu, 2020. *SafyID* [online]. Buchlovice: COMFIS s.r.o. [cit. 2020-09-21]. Dostupné z: https://www.safyid.com/otisk-prstu/

Population.City, 2015. *City populations worldwide* [online]. population.city [cit. 2020-09-06]. Dostupné z: http://populace.population.city/world/#1

Postižení oční sítnice může znamenat i trvalé poškození zraku (Ordinace.cz), 2014. *Eseznam.cz* [online]. Třinec: Evropský spolek pro OZP [cit. 2020-09-06]. Dostupné z: http://www.eseznam.cz/index.php/rubriky/ruzne-clanky/3003-postizeni-ocni-sitnice-muze-znamenat-i-trvale-poskozeni-zraku?jjj=1599400366101

RADEK BENEŠ [online], 2013. Praha: Radek Beneš [cit. 2021-01-24]. Dostupné z: https://radek-benes.cz/clanky/prolomeni-hesla-hrubou-silou.html

RAK, Roman, 2008e. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 318-342. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, 2008f. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 113. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, 2008g. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 114-115. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, 2008h. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 116-117. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman a Václav MATYÁŠ, 2008i. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 117-1118. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA, 2008b. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 106. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA, 2008c. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 473-474. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA, 2008d. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 210-230. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA, 2008j. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 135-139. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA, 2008k. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 140. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Václav MATYÁŠ a Zděněk ŘÍHA, 2008a. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, s. 89. Profesionál. ISBN 978-80-247-2365-5.

RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA, 2008l. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada. Profesionál. ISBN 978-80-247-2365-5.

SLANINOVÁ, TEREZA, Gabriela BRONCOVÁ, Jiří STRAUS a Tatiana SHISHKANOVA, 2019. VIZUALIZACE DAKTYLOSKOPICKÝCH STOP POMOCÍ VODIVÝCH POLYMERŮ. *Chemické listy*. **113**(9), 532. ISSN 1213-7103.

ŠVARC, Dan, 2001. Jak si stojí české internetové bankovnictví?. *Měšec.cz* [online]. Praha: Měšec.cz [cit. 2020-09-06]. Dostupné z: https://www.mesec.cz/clanky/jak-si-stoji-ceske-internetove-bankovnictvi/

VEJNAR, Jiří, 2001. *Homebanking: Do každé domácnosti i kanceláře*. Praha.

8 Přílohy

Příloha A Základy bezpečnosti na Internetu

Příloha A Základy bezpečnosti na Internetu

Základy bezpečnosti na Internetu

RNDr. Václav Hník, CSc., Mgr. Oldřich Krulík, Ph.D., Mgr. Eva Staňová
Ministerstvo vnitra, odbor bezpečnostní politiky

Internet umožňuje rychlou a relativně anonymní výměnu informací a názorů. Tím slouží jak legálním účelům, tak zločincům, včetně teroristů. Ti mohou jeho prostřednictvím šířit svou propagandu a oslovovat sympatizanty. Jak teroristé, tak vyzvědači nebo zločinci, vedení zištnými pohnutkami, mohou v rámci Internetu rozesílat viry. To jsou programy, které mohou poškodit, změnit nebo zničit určitá data, případně umožní přístup k údajům uvnitř konkrétního systému. V důsledku takového počínání může dojít i k poruchám zařízení kritické infrastruktury, jejichž některé ovládací systémy jsou propojeny se sítí Internet.

- Aniž by musela být řeč rovnou o „kybernetickém terorismu" nebo špionáži, je obecně vhodné dodržovat základní pravidla bezpečnosti na Internetu, která Vám mohou mimo jiné ušetřit nemalé finanční prostředky či řadu dalších komplikací, spojených se ztrátou či nechtěným zveřejněním konkrétních dat.
- Následující rady jsou určeny primárně těm, kteří jsou připojeni k síti Internet, ale využít jich částečně mohou i ostatní uživatelé informačních a komunikačních technologií.

Pravidla všeobecné prevence:

- Nikdy o sobě v rámci internetové komunikace bezdůvodně nesdělujte zneužitelné informace (adresu bydliště, telefon, číslo kreditní karty, e-mailovou adresu, heslo e-mailu a podobně).
- Používejte výhradně legální software. Dávejte důsledný pozor na pochybné hry a jiné programy, nabízené zdarma (freeware, shareware, utilities).
- Nezapojujte se do jakéhokoli nelegálního dění na Internetu (stahování či sdílení nelegálního software včetně hudby, videa a pornografie).
- Nikdy neotevírejte soubory přiložené k elektronickým zprávám (e-mailům) od Vám neznámých osob. Zpravidla se jedná o nevyžádanou reklamu (spam), pokud ne přímo o viry.
- Užívejte účinné antivirové programy a dostatečně často je aktualizujte.
- Informace z externích zdrojů (e-mail, CD-ROM, DVD, diskety, USB média) vždy kontrolujte antivirovým programem. Pravidelně kontrolujte i celý obsah pevného disku.
- Zvláštní nebezpečí znamenají spustitelné programy (zejména – ale nikoli výlučně – se jedná o koncovky *.exe, *.com a *.bat). Nenechte se zmýlit používáním tzv. dvou přípon souborů. Skutečná přípona je ta, která je zcela na konci souboru (tj. soubor „obrazek.jpg.exe" není obrázek, ale program, a to s největší pravděpodobností virus).
- Dávejte bedlivý pozor na možné přesměrování (re-dial). Pečlivě prostudujte aktivní okna některých internetových stránek, která Vám dávají na vybranou mezi „ano" a „ne". Někdy i obě volby mohou znamenat, že se Vaše účty za připojení vyšplhají do astronomických výšek. V takovém případě vypněte nejen konkrétní okno (křížek v pravém horním rohu), ale raději i celý prohlížeč.
- Pravidelně, například jednou měsíčně, zálohujte důležitá data (vypálením na CD-ROM, atd.).
- Nepouštějte ke svému počítači osoby, které nejsou ochotny dodržovat bezpečnostní pravidla (to platí i o vlastních příbuzných).
- Svůj počítač chraňte i dostatečně komplikovanými a často obměňovanými hesly.
- Dbejte i na fyzickou ochranu výpočetní techniky a dat (v odůvodněných případech to může znamenat i náležité stavební úpravy, kvalitní dveře s bezpečnostním zámkem, bezpečnostní fólie a mříže na oknech, poplachové zařízení, atd.).
- Chraňte příslušná data před dětmi. Zamezte jejich přístupu na pornografické, extremistické a další nežádoucí stránky.
- Jestliže na Internetu naleznete něco, o čem jste přesvědčeni, že je to nelegální (extremistická propaganda, dětská pornografie, návody na výrobu improvizovaných zbraní) ohlaste tuto skutečnost Policii České republiky.

Možnosti rozpoznání viru v osobním počítači:

- Na výskyt viru Vás upozorní antivirový program.
- Svou přítomnost někdy virus oznámí sám, tzv. „hláškou" na obrazovce.
- Na virus Vás upozorní ta skutečnost, že přestanou fungovat určité programy nebo počítač zkolabuje jako celek.

- Ani samo zjištění viru v počítači nemusí být vždy přímo důvodem k panice.
- Pokud zjistíte, o jaký virus se konkrétně jedná (to Vám zpravidla oznámí Váš antivirový program), pokuste se na Internetu najít (nejlépe pomocí jiného počítače, než nakaženého) jeho účinky a nejvhodnější způsob „léčby".
- Pokud komplikace trvají, obraťte se na někoho informovanějšího, případně přímo na specializovanou firmu.

Z dalších zdrojů informací Vám doporučujeme:

- http://www.bezpecneonline.cz/:chraňte sebe, svůj počítač a firmu před nástrahami na Internetu (Ministerstvo informatiky)
- http://www.egovernment.cz/archiv/pdf 3-06/1.pdf: pravidla bezpečnosti elektronické komunikace (magazín E-Government)
- http://www.myslenka.cz/: více k tématu ochrany duševního vlastnictví (iniciativa „Právo na straně myšlenky")
- http://www.zatepla.cz/: více k tématu bezpečného Internetu a legálního software (server "zatepla.cz")
- http://www.bsa.org/czechrepublic/: více k tématu bezpečného Internetu a legálního software (Business Software Alliance)
- http://www.cpufilm.cz: Česká protipirátská unie;
- http://www.filmynejsouzadarmo.cz: více k tématu ochrany duševního vlastnictví
- http://www.itpravo.cz/: server o právních a bezpečnostních otázkách, spojených s informačními technologiemi.
- http://www.mojebanka.cz/cs/security.shtml: desatero bezpečnosti Komerční banky, a. s.
- http://www.csas.cz/banka/content/inet/internet/cs/standard_content_pi01_005001.xml: Internetbanking, Česká spořitelna a. s.
- http://www.citibank.cz/czech/consumer-banking/czech/files/phish_cz.pdf: rady pro bezpečné internetové bankovnictví (Citibank)

Zdroj: (Hník, 2020)