Západočeská univerzita v Plzni

Fakulta aplikovaných věd

Katedra informatiky a výpočetní techniky

Diplomová práce

Perspektivní bezpečnostní metody pro přímé bankovní kanály

Plzeň 2012 Bc. Jakub Kučera

Prohlašuji, že jsem diplomovou práci vypracoval samostatně pod vedením Doc. Jany Klečkové a uvedl v seznamu literatury všechny použité literární a odborné zdroje.

V Plzni dne X.Y.2012 _____

vlastnoruční podpis autora

Abstrakt

Tato práce si klade za cíl analyzovat a porovnat klasické i moderní autentizační metody využitelné pro oblast internetového, mobilního bankovnictví a klientských portálů jako jsou například čipové karty, risk-based systémy, biometrie. Kromě autentizačních metod je zaměřena na moderní bezpečnostní metody, kterou může být například detekce anomálií. První část obsahuje porovnání jednotlivých autentizačních metod z několika hledisek (úroveň bezpečnosti, soulad s legislativou, uživatelský komfort apod.). V druhé části je uveden návrh metody pro monitorování uživatele s využitím technologie JBoss Drools, kterou lze nasadit v reálném prostředí.

Abstract

This work aims to analyze and compare classic and modern authentication methods which are useful for internet, mobile banking and client portals, like for example chip cards, risk-based systems and biometrics. In addition to authentication methods this work is focused on the modern security methods, like anomaly detection. First part of work contains comparing of various authentication methods from several aspects (level of security, compliance, comfort for user etc.). The second part provides method of user security monitoring in real environment using the JBoss Drools.

Obsah

1. Úvod

Přímé (neboli elektronické) bankovnictví se v dnešní době stává díky dynamickému vývoji v oblasti internetu, mobilních telefonů, osobních počítačů a ostatních informačních technologií pevnou součástí všech bankovních institucí. Některé bankovní instituce jsou přímo na tomto druhu bankovnictví založeny a využívají tak výhody elektronického bankovnictví v plném měřítku.

S vývojem v oblasti informačních technologií a všeobecné dostupnosti internetu vznikají nové kanály pro zprostředkování elektronického bankovnictví. Zároveň však také stoupá nebezpečí zneužití. V reakci na zvyšující se nároky na bezpečnost vznikají nové moderní autentizační metody. Tyto metody přinášejí vyšší bezpečnost, ale při jejich zavedení do praxe je nutné se zabývat i ostatními faktory, jež tyto metody přinášejí (finanční náročnost, uživatelská přívětivost).

Tak jako vznikají nové autentizační metody tak i v oblasti prevence zneužití identity a detekce útoků jsme mohli zaznamenat velký pokrok. Například detekce podezřelého chování uživatele je v dnešní době považována za jednu z klíčových metod v oblasti zabezpečení bankovnictví.

První část práce je věnována popisu kanálů přímého bankovnictví s vysvětlením nejdůležitějších pojmů a stručným přehledem možných útoků a zneužití v této oblasti. V další části uvedu moderní autentizační metody s jejich výhodami a nevýhodami.

Praktickou část tvoří analýza vlastností vybraných autentizačních metod z několika hledisek a návrh systému pro analýzu chování uživatele elektronického bankovnictví využívající technologii JBoss Drools.

2. Teoretická část

2.1. Přímé bankovnictví

Elektronické bankovnictví lze definovat jako poskytování bankovních služeb a plateb prostřednictvím bankovního systému elektronickou cestou [AP].

Elektronické (neboli přímé) bankovnictví, se v poslední dekádě stalo nedílnou součástí služeb poskytovaných bankovními ústavy. V době svého vzniku bylo považováno za přímého nástupce konvenčního způsobu užívání bankovních služeb, nicméně tento pohled se ukázal jako příliš optimistický – stále mnoho zákazníků zůstává konzervativních a raději dává přednost klasickým metodám. Přesto stále rostoucí podíl přímého bankovnictví v celkovém souhrnu využití bankovních služeb ukazuje, že je tato forma zprostředkování bankovních služeb velkým příslibem do budoucna.

2.1.1. Historie přímého bankovnictví

Za vznik elektronického bankovnictví je nejčastěji považován rok 1914, kdy ve Spojených státech amerických vydala společnost Western Union Telegraph Company první debetní kartu vyrobenou z plechu. Umožňovala zákazníkům bezhotovostně posílat telegramy a volat. Vždy na konci měsíce byl zákazníkům zaslán výpis (jakési vyúčtování) za poskytnuté služby a zákazník pak již tuto částku uhradil klasickou cestou (šekem, příkazem na pobočce banky apod.).

V roce 1950 společnost Diners Club International vydala pro vybraných 200 zákazníků první univerzální kartu (tzv. Charge Cards) pro bezhotovostní platbu v síti hotelů a restaurací této společnosti.

Opravdovým milníkem na poli elektronického bankovnictví se stala 80. léta, kdy čtyři největší New Yorské banky (Citibank, Chase Manhattan, Chemical and Manufacturers Hannover) začaly nabízet homebanking. Jejich nabízené systémy bohužel nepřesvědčily dostatečné množství zákazníků a tak od nich bylo postupně upuštěno [MJC]. Přesto se právě bankovní sektor stal jedním z největších zákazníků pro nové informační technologie a nástup internetu, jako komunikačního prostředku dostupného komukoli, dal za vznik první, čistě internetové banky, kterou byla v roce 1995 americká First Network Bank.

V dnešní době již v České republice existuje několik internetových bank, a zároveň ostatní bankovní instituce nabízejí internetové bankovnictví součást svého přímého bankovnictví.

2.1.2. Kanály přímého bankovnictví

2.1.2.1. Homebanking

Homebanking, domácí nebo také počítačové bankovnictví je druh přímého bankovnictví, kdy klient má ve svém počítači nainstalován software dodaný bankovním institutem. Pomocí tohoto software pak může klient spravovat své účty.

Tento druh přístupu k bankovnictví zaznamenal největší růst počátkem 90. let, kdy nebyl internet na takové technické úrovni jako nyní (zejména z hlediska dostupnosti a přenosových kapacit), přesto bylo nutné zákazníkům nabídnout službu, která by umožnila spravovat účty bez nutnosti osobní návštěvy na pobočce.

S nástupem vysokorychlostního a dostupného internetu je homebanking postupně nahrazován internetbankingem, stále si ovšem zachovává velké množství zákazníků, především z firemní oblasti. Důvodem je možnost snadno pracovat s velkým množstvím formulářů a v neposlední řadě také dovoluje propojení s firemními informačními systémy.

Přenos přes šifrovaný kanál SSL a autentizace pomocí certifikátů zajišťuje celkovou bezpečnost komunikace mezi klientským softwarem a bankovní institucí.

2.1.2.2. Internetbanking

Internetbanking patří mezi nejpoužívanější formy přímého bankovnictví. Přináší stejné výhody jako homebanking, ale oproti němu není zapotřebí speciálního softwaru na straně klienta. K plnohodnotnému používání internetového bankovnictví stačí klientovi pouze internetové připojení a prohlížeč.

Díky jednoduchosti používání a širokému portfoliu nabízených služeb, které je u některých bankovních institucí téměř rovnocenné s nabídkou v kamenných pobočkách, roste počet uživatelů internetového bankovnictví velmi rychle. Jak je vidět na následující tabulce [STA], celkový počet obyvatel, kteří využívají internetového bankovnictví se za posledních 7 let téměř zešestinásobil.

Rok	2005	2008	2009	2010	2011
Počet obyvatel v procentech	**5,2**	**13,4**	**17**	**21**	**27,4***
*** předběžný údaj**					

Tabulka 1: Počet obyvatel využívajících internetové bankovnictví v ČR

Bezpečnost přenosu je stejně jako u homebankingu zajištěna komunikací přes zabezpečený kanál pomocí SSL. Další způsoby zabezpečení internetového bankovnictví jsou u jednotlivých bankovních institucí odlišné. Například Česká spořitelna nabízí několik možností jak autentizovat uživatele v internetovém bankovnictví. První metodou je klasické použití uživatelského čísla a hesla, dalším pak přihlášení pomocí certifikátu na čipové kartě nebo je možné využít autentizační kalkulátor.

2.1.2.3. Mobilní bankovnictví

Rozvoj mobilního bankovnictví, stejně jako ostatní druhy přímého bankovnictví, úzce souvisel s vývojem technologií (dostupností GSM sítí, vývojem telefonů). Počátky se datují od poloviny 90. let.

Princip mobilního bankovnictví spočívá v komunikaci klienta s bankovní institucí prostřednictvím mobilního telefonu. Existuje několik forem mobilního bankovnictví, které budou popsány dále.

2.1.2.3.1 SMS banking

SMS banking je nejjednodušší forma mobilního bankovnictví. Využívá se zasílání přesně definovaných SMS zpráv (právě pevně daná struktura je jednou z hlavních nevýhod tohoto kanálu, neboť snadno dochází k překlepům, které mohou mít někdy i závažné důsledky). SMS banking používá techniky PUSH & PULL zpráv.

Metoda PUSH znamená, že klient nijak neiniciuje komunikaci s bankou, ale ona sama (resp. bankovní aplikace skrze SMS server) posílá zprávy klientovi. Zpravidla se jedná o zprávy informačního typu (pravidelný výpis účtu, ohlášení stavu transakce).

Při metodě PULL naopak klient iniciuje komunikaci a posílá požadavek na bankovní aplikaci (například příkaz k úhradě).

Díky 24 hodinové dostupnosti a faktu, že GSM v dnešní době disponuje téměř jakýkoli mobilní telefon, patřilo sms bankovnictví mezi oblíbené metody. V současnosti ovšem i díky mobilním aplikací spíše skomírá.

2.1.2.3.2 SIM Toolkit

Technologie SIM Toolkit spočívá ve speciálním softwaru, nahraném na k tomuto účelu upravenou SIM kartu, a který zprostředkovává komunikaci mezi klientem a bankou. Komunikace probíhá zasíláním automaticky generovaných SMS zpráv, které jsou šifrovány. Právě díky nainstalovanému softwaru je práce klienta v mnoha ohledech zjednodušena (např. nemusí znát přesný formát zpráv, protože jsou automaticky generovány).

Mobilní bankovnictví využívající SIM Toolkit dnes nabízejí téměř všechny bankovní instituce v České republice.

2.1.2.3.3 WAP banking

Tento druh bankovnictví využívá technologie WAP. Můžeme si jej představit jako zjednodušenou formu internetového bankovnictví v mobilním telefonu. Přístup ke správě účtu probíhá přes wapový prohlížeč v telefonu komunikací protokolem WAP.

Kvůli svému ne zcela přívětivému uživatelskému rozhraní, velkým přenosovým objemům a v neposlední řadě také finanční náročnosti, bývá WAP banking nahrazován modernějšími metodami mobilního bankovnictví.

2.1.2.3.4 Java klientské aplikace

Použití jazyka Java v mobilním bankovnictví nabídlo klientům banky možnost používat téměř všechny bankovní operace ve svém mobilním telefonu. Navíc díky technologii jazyka Java přináší velmi přívětivé uživatelské rozhraní a stalo se tak přímým následníkem WAP bankingu.

Klient pomocí Java aplikace, která je poskytnuta bankou, spravuje svůj bankovní účet prostřednictvím datového spojení (například GPRS, EDGE, nebo 3G).

V České republice tento způsob bankovnictví nabízí pouze Komerční banka (aplikace Mobilní banka) a UniCredit Bank (aplikace SmartBanking).

2.1.2.4. Telefonní bankovnictví

Telefonní bankovnictví bylo jedním z prvních kanálů přímého bankovnictví. Mezi hlavní přednosti patří relativně velká dostupnost (všechny bankovní instituce mají svá call centra, k volání stačí jakýkoli telefon) a široká nabídka služeb a informací (díky osobnímu kontaktu s operátorem). Naopak největší nevýhodou tohoto druhu bankovnictví je jeho finanční náročnost (jak na straně klienta z pohledu vysoké ceny za hovor, tak i ze strany bankovní instituce kvůli vysokým nákladům na provoz).

Můžeme jej rozdělit na dvě skupiny. První skupinou je použití call centra, kdy klient přímo komunikuje s operátorem v bance, který plní jeho požadavky. Druhou skupinu pak tvoří systém IVR (*Interactive voice response*), kdy klient komunikuje s telefonním automatem prostřednictvím tzv. tónové volby.

Většina bankovních institucí v České republice nabízí své vlastní řešení telefonního bankovnictví, které je obvykle kombinací obou zmíněných způsobů přístupu.

2.2. Bezpečnost přímého bankovnictví

Bankovní instituce vkládající své prostředky do zabezpečení svých i klientských prostředků proti fyzickému napadení (budování vysoce zabezpečených bankovních trezorů, střežené převozy peněz) musejí díky velkému nárůstu počtu klientů využívajících služeb přímého bankovnictví investovat do zabezpečení těchto kanálů a nabízet svým klientům vždy nejvyšší možnou úroveň zabezpečení jejich prostředků, avšak tato úroveň nesmí mít vliv na uživatelskou přívětivost při práci s jakýmkoli kanálem přímého bankovnictví.

V této kapitole popisuji nejdůležitější termíny a metody používané k zabezpečení přímých bankovních kanálů. Dále jsou zde uvedeny nejčastější typy útoků na přímé bankovnictví. Poslední část této kapitoly je věnována moderním bezpečnostním metodám přímého bankovnictví.

2.2.1. Základní termíny

V oblasti bezpečnosti v bankovnictví jsou nejčastěji uváděny tyto tři základní pojmy [MŘ]:

- ***Autentizace*** – proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky).
- ***Autorizace*** – udělení určitých práv a určení povolených aktivit.
- ***Identifikace*** – rozpoznání určité entity (systémem) v dané množině entit.

Termíny identifikace a autentizace bývají v praxi často zaměňovány. Identifikace znamená, že osoba se nějakým způsobem identifikuje vůči systému (jiné osobě atd.), to znamená, že podává o sobě určité informace (například zadá své uživatelské jméno). V odborné literatuře je identifikace často označována jako odpověď na otázku „Kdo jsem?“ či „O koho jde?“. Oproti tomu autentizace je, jak již bylo výše zmíněno, proces ověření identity. Tedy jde o ověření, zda je osoba opravdu tou, za kterou se vydává.

2.2.2. Šifrování dat

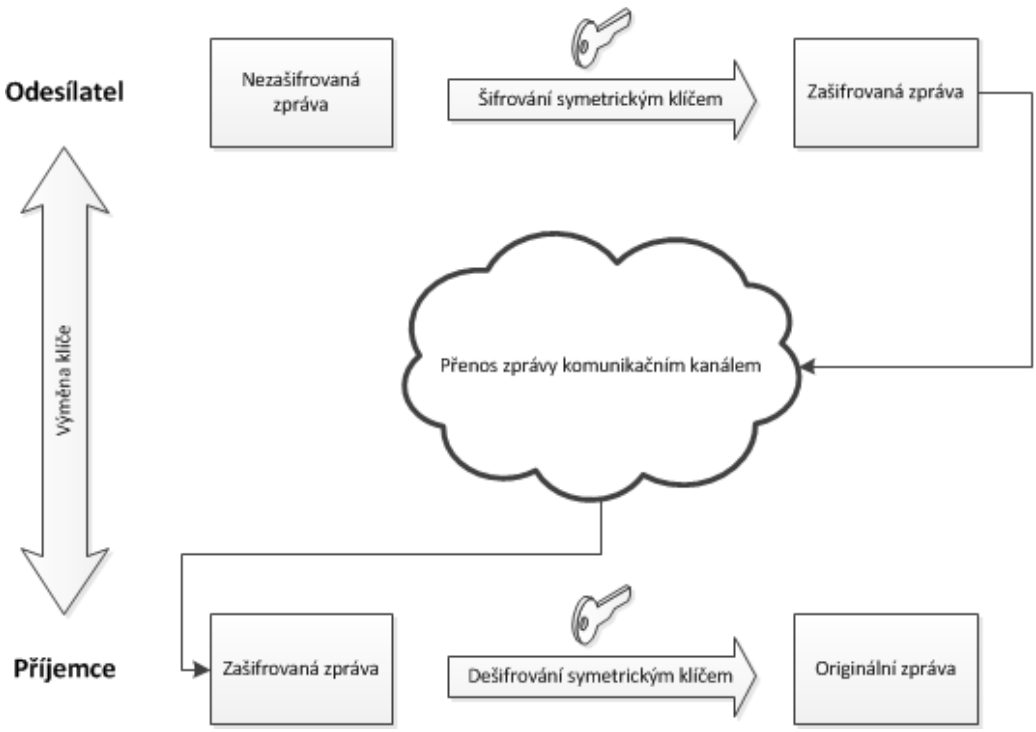
Šifrováním je označen proces transformace originální informace (nazývána jako tzv. plaintext) do transformované informace, zvané šifrovaný text, která má obvykle náhodnou, nesrozumitelnou podobu. Takto transformovaná informace se nazývá kryptogram, neboli šifrovaný text [LRG].

Důvodem použití šifrování je zabránění zveřejnění originální informace při jejím přenosu komunikačním kanálem. Abychom mohli informaci zašifrovat a na opačném konci komunikačního kanálu ji opět převést do smysluplné podoby, je nutné mít k dispozici speciální znalost a sice šifrovacího (resp. dešifrovacího) klíče.

Existují dva základní přístupy k šifrování dat, symetrické a asymetrické šifrování, které se liší počtem používaných klíčů, šifrovacími algoritmy a oba mají samozřejmě své výhody a nevýhody.

2.2.2.1. Symetrické šifrování dat

Charakteristickým rysem symetrického šifrování je využití pouze jednoho klíče, a to jak na straně odesílací (tj. při šifrování zasílané informace) tak i na straně přijímací (dešifrování). Odesílatel tedy informaci zašifruje pomocí klíče a příjemce tuto zašifrovanou informaci dešifruje použitím toho samého klíče. Tento princip sebou ovšem přináší nutnost znalosti klíče před počátkem komunikace na obou jejích koncích. Tudíž je nutné nějakým bezpečným způsobem přenést klíč mezi oběma komunikujícími objekty. Algoritmy využívající symetrické šifrování jsou například 3DES, RC4, AES, IDEA a mnoho dalších.

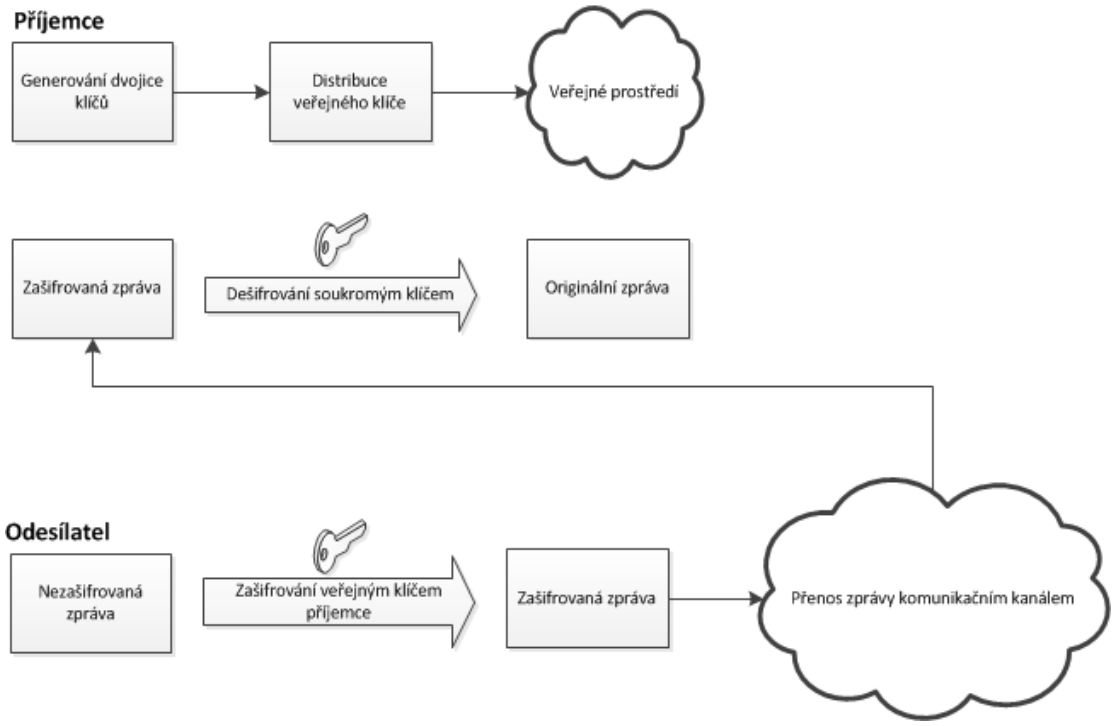


Obrázek 1: Princip symetrického šifrování

2.2.2.2. Asymetrické šifrování dat

Asymetrické šifrování používá vždy dvojici klíčů, soukromý a veřejný. Základní princip této metody je následující:

1. Příjemce vygeneruje dvojici klíčů, veřejný klíč (VK_p) potom distribuuje všem.
2. Odesílatel šifruje zprávu pomocí VK_p a odešle ji příjemci.
3. Příjemce přijatou zprávu dešifruje použitím svého soukromého klíče.



Obrázek 2: Princip asymetrického šifrování

Tento druh šifrování využívá skutečnosti, že je relativně jednoduché veřejným klíčem zprávu zašifrovat, ale téměř nemožné pouze na základě znalosti veřejného klíče zašifrovanou zprávu dešifrovat. Ovšem existují typy útoků, které i pro tento druh šifrování představují nebezpečí. Popisem útoků se věnuje kapitola 2.2.4.

Nejčastěji používaným algoritmem pro asymetrické šifrování je algoritmus RSA, který nahradil DSA. Za zmínku ovšem také stojí algoritmus eliptických křivek, neboli ECC (*Elliptic Curve Cryptography*), která nabízí při srovnatelné úrovni bezpečnosti kratší klíče a je tudíž vhodný pro mobilní bezdrátová zařízení jakou jsou například čipové karty.

K největším nevýhodám asymetrického šifrování patří zejména velká časová náročnost. V literatuře je uváděno, že asymetrické šifrování je asi 1000 krát pomalejší než symetrické.

2.2.3. Elektronický podpis

Elektronickým podpisem jsou dle znění zákoníku [ZA] míněné údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.

Zmíněný zákoník dále zavádí termín **zaručený elektronický podpis**, který splňuje následující požadavky:

1. Je jednoznačně spojen s podepisující osobou.
2. Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
3. Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
4. Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Jak již ze samotného názvu vyplívá, zaručený elektronický podpis nám dává jisté záruky. Konkrétně jeho použitím lze ověřit, zda nedošlo k porušení obsahu zprávy (samotná přítomnost elektronického podpisu změně nezabrání). Také nám umožňuje jednoznačně identifikovat podepsanou osobu.

Dalším používaným termínem je takzvaný **uznávaný elektronický podpis**. Jedná se o druh elektronického podpisu, který je obecně uznáván, například na úřadech. Na rozdíl od zaručeného podpisu je kladen velký důraz na zjištění a vyjádření identity podepsané osoby. To znamená, že nemůže existovat uznávaný elektronický podpis, který by identifikoval například smyšlenou postavu.

Nejčastější implementací elektronického podpisu je digitální podpis. Existují i jiné metody použití elektronického podpisu, např. biometrické, ty ale se ale příliš často v bankovních kanálech nepoužívají.

2.2.3.1. Digitální podpis

V literatuře se často zaměňují pojmy elektronický a digitální podpis. Elektronický podpis značí jakousi globální abstrakci, která neuvádí žádnou konkrétní technologii. Zatímco digitální podpis už je konkrétní implementace elektronického podpisu a v praxi je tedy digitální podpis zaručeným elektronickým podpisem.

Digitálním podpis zaručuje tři hlavní bezpečnostní aspekty. Jsou jimi **integrita, identifikace** a **nepopíratelnost**.

Integritou je myšleno neporušení obsahu zprávy. Digitální podpis ovšem sám o sobě nezaručí neporušení obsahu, ale dovolí tuto změnu jednoznačně identifikovat.

Digitální podpis umožňuje identifikaci podepsané, respektive podepisující osoby. Například se jedná o údaje typu jméno a příjmení.

Nepopíratelnost označuje fakt, že podepsaná osoba nemůže popřít, že právě ona tento podpis vytvořila.

Princip digitálního podpisu využívá asymetrického šifrování s speciální funkcí zvanou hash. Pro snížení paměťových i výpočetních nároků, které by byly při asymetrickém šifrování celé zprávy velmi vysoké je vytvořen otisk zprávy. Otisk se následně zašifruje soukromým klíčem osoby, která digitální podpis vytváří. Takto zašifrovaný otisk připojí ke zprávě, kterou následně zašifruje veřejným klíčem příjemce. Příjemce dešifruje zprávu svým soukromým klíčem. Veřejným klíčem odesílatele potom provede hash dešifrované zprávy a porovná ho s otiskem přiloženým ke zprávě. Pokud se shodují je jasné, že zpráva nebyla modifikována.

Hash je název pro jednocestnou funkci, tj. funkci kterou lze snadno vypočítat, ale je velmi obtížné (téměř nemožné) z jejího výsledku odvodit vstup funkce. Nejčastěji používanými algoritmy hashovací funkce jsou MD5, SHA-1 a SHA-2.

Oproti šifrování využívá digitální podpis předpokladu, že operace šifrování a dešifrování jsou zaměnitelné. Tedy zpráva je zašifrována veřejným klíčem a lze ji dešifrovat klíčem soukromým a stejně tak i obráceně.

2.2.3.2. Certifikát

Certifikátem je označena datová struktura, která obsahuje veřejný klíč osoby a její identifikační údaje. Dalšími údaji obsaženými v certifikátu jsou verze a pořadové číslo certifikátu, algoritmus podpisu, platnost, jméno vydavatele certifikátu a další rozšiřující údaje.

Formát certifikátu určuje několik mezinárodních norem. K nejpoužívanější patří X.509, konkrétně ve verzi 3. Vydavatelem certifikátu je tzv. certifikační autorita (dále jen CA), která zaručuje integritu vydávaných certifikátů (tedy ručí za to, že veřejné certifikáty nejsou podvržené).

Princip získání certifikátu je následující: Osoba si nejprve vygeneruje dvojici klíčů a vyplní žádost o certifikát (doplní údaje o své osobě, popř. další požadované informace). Tuto žádost pak digitálně podepíše svým soukromým klíčem – důkaz o vlastnictví soukromého klíče. CA ověří totožnost osoby a verifikuje podpis na přijaté žádosti. Pokud skončí verifikace v pořádku, CA vystaví nový certifikát a předá jej žadateli.

V České republice jsou akreditovány tři certifikační autority: Česká pošta s.p., První certifikační autorita a.s. a eIdentity a.s.

Práci s certifikáty a jejich přenos, potvrzování zajišťuje infrastruktura PKI (*Public key infrastructure*). PKI zahrnuje především tyto části:

- **CA** - Certifikační autoritu – viz výše
- **RA** - Registrační autoritu – verifikují identitu uživatel při komunikaci s CA
- **Úložiště** – bezpečné úložiště klíčů
- **Systém pro management certifikátů**

2.2.4. Ohrožení přímého bankovnictví

S pokračujícím vývojem informačních technologií a rostoucím objemem finančních toků představuje přímé bankovnictví lákavý cíl pro potencionální útoky. Právě díky nejnovějším technologiím je takový útok pro útočníka poměrně snadný a přináší mu oproti fyzickému útoku nesporné výhody, zejména malou pravděpodobnost odhalení a relativní jednoduchost útoku.

Úměrně s rostoucím počtem bankovních kanálů rostou i možnosti pro potenciální útok. Stejně tak stále se zdokonalující bezpečnostní metody zapříčiňují vznik nových a komplexnějších útoků. Tento souboj ve svém konečném důsledku pak způsobuje fakt, že na poli bezpečnosti vznikají v rychlém časovém sledu stále nová a bezpečnější řešení a vývoj v této oblasti směřuje rychle kupředu.

Druhů útoků na přímé bankovnictví existuje obrovské množství, v následujících kapitolách uvedu pouze nejčastější typy útoků.

2.2.4.1. MITM – Man in the Middle

Z anglického „člověk uprostřed“. Patří mezi nejznámější typy útoků. Jeho princip je velice jednoduchý. Útočník se snaží odposlouchávat komunikaci mezi účastníky takovým způsobem, aby se mohl stát aktivním prostředníkem, který může odposlouchanou komunikaci modifikovat či jinak zneužít, přičemž ostatní účastníci se domnívají, že komunikují napřímo.

Existuje zde i riziko tzv. otrávení DNS cache (tzv. *DNS poisoning*), kdy útočník vloží vlastní DNS záznam do cache DNS serveru, a uživatel pak bude přesměrován na podvržený server, na kterém bude stejná přihlašovací obrazovka, jakou uživatel zná ze svého internetového bankovnictví. Známý je také útok zvaný ARP spoofing, který využívá podvržení MAC adresy.

Útok MITM existuje v mnoha modifikacích. Například Man in the Mobile, který spočívá v nasazení malware[1] do mobilního telefonu a podvržení mTAN[2] tak, aby napadený

[1] Malware – krátký program, určený ke vniknutí, nebo poškození systému
[2] mTAN – *mobile Transaction Authentication Number* – jedna z forem jednorázového hesla používaném v mobilním bankovnictví

uživatel nepoznal, že mTAN je vygenerován k úplně jinému účtu a částce než pro kterou vytvořil příkaz. Dalším příkladem MITM útoku je Man in the Browser. V něm se stává prostředníkem infikovaný webový prohlížeč, který může měnit webové stránky, obsahy transakcí, nebo přidávat další transakce, přičemž uživatel a ani webová aplikace na straně poskytovatele nemusí mít o ničem tušení.

2.2.4.2. Phishing

Phishing se i díky mediální pozornosti stal na poli útoků na přímé bankovnictví fenoménem. Nicméně i přes značné všeobecné povědomí o tomto druhu útoku a jeho principu, se jeho iniciátoři stále setkávají s úspěchem.

Principem útoku je rozeslání velkého množství zpráv (nejčastěji emailových), které vyzívají příjemce k zadání citlivých údajů. Zprávy mají takovou podobu, aby příjemce nabyl vědomí, že pocházejí z renomovaných (příjemci známých) webových serverů (ať už to jsou bankovní instituce, aukční portály aj.). Někdy také oslovují příjemce sdělením, že právě on se stává vítězem určité ceny a pro výhru stačí zadat několik údajů. Popřípadě zprávy obsahují odkaz na stránky falešného internetového bankovnictví, které jsou téměř identické s pravými, a iniciují uživatele k zadání přihlašovacích údajů.

Phishing bývá úspěšný zejména kvůli vysokému počtu odeslaných zpráv, kdy alespoň malé množství příjemců se „*chytí*“. Odtud pochází samotný název, který vychází z anglického „*fishing*“ neboli rybaření.

2.2.4.3. Pharming

Pharming je velmi podobný phishingu. Používá již zmíněného DNS cache poisoning. Uživatele podvržený DNS záznam přesměruje na stránky, která jsou téměř identické internetovému bankovnictví, jež uživatel běžně používá, a přiměje ho k zadání přihlašovacích údajů, která jsou poté zneužity.

Samotná změna záznamu se může provést buď v tzv. *hosts*[3] souboru na systému uživatele, nebo také změnou DNS záznamů ve směrovačích, ke kterým je uživatel připojen.

[3] Hosts soubor - soubor, ve kterém je formou textu nastaveno mapování mezi hostname a IP adresami

2.2.4.4. Key logger

V tomto případě útoku (keylogging) je na uživatelský systém nasazen škodlivý software (v některých případech může být útok realizován i hardwarově), který následně odposlouchává a zaznamenává stisknuté klávesy. Takto získané záznamy stisku kláves jsou poté poslány útočníkovy, který z nich může získat citlivé údaje o uživateli.

2.3. Bezpečnostní metody v přímých bankovních kanálech

Cílem této kapitoly je seznámit čtenáře se základními a moderními bezpečnostními metodami v oblasti přímého bankovnictví. První část je věnována autentizaci a autentizačním metodám. Dále jsou zde uvedeny další bezpečnostní metody, jako například risk-based systémy, nebo metoda bezpečnostního monitoringu.

2.3.1. Autentizace

Jak již bylo zmíněno dříve, autentizace je proces ověření identity uživatele. Samotné autentizační metody lze pak rozdělit do tří základních faktorů:

- Uživatel něco ***zná*** – PIN, heslo aj.
- Uživatel něco ***má*** – čipová karta, kreditní karta
- Uživatel něčím ***je*** – biometrické vlastnosti (podpis aj.)

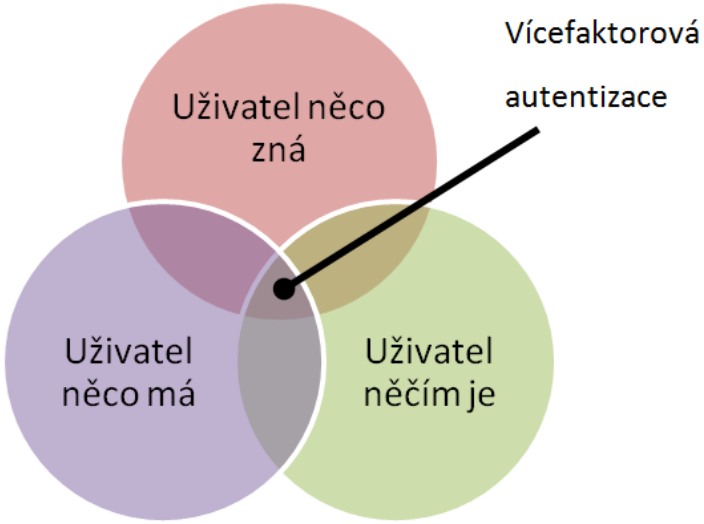
Jednotlivé faktory mají své výhody i nevýhody, přičemž platí, že čím více těchto faktorů obsahuje autentizace, tím je menší pravděpodobnost kompromitace.

Jednofaktorovou autentizací může být například přihlášení k emailovému účtu, kdy uživatel zadá své ID a heslo, tedy pouze ty parametry, které uživatel **zná**. Oproti tomu při výběru z bankomatu je použita dvoufaktorová autentizace, neboť uživatel nejprve vloží svou kreditní kartu, tj. něco **má**, a poté zadá svůj PIN, tj. něco co **zná**.

Z hlediska bezpečnosti je použití vícefaktorové autentizace klíčové. Bohužel některé finanční instituce buď vícefaktorovou autentizaci nenabízejí, nebo špatně pochopili její význam. Dle [FFIEC] lze vícefaktorovou autentizaci definovat takto (volně přeloženo):

Dle definice, pravá vícefaktorová autentizace spočívá v použití dvou nebo více řešení ze tří skupin faktorů. Použití více řešení ze stejné kategorie na různých místech autentizačního procesu může být součástí vrstvené bezpečnosti nebo jiných metod řízení přístupu, avšak toto nepředstavuje vícefaktorovou autentizaci.

Na Obrázek 3 je zřetelně znázorněna oblast, která představuje vícefaktorovou autentizaci.



Obrázek 3: Vícefaktorová autentizace

Společnost RSA uvádí i čtvrtý autentizační faktor [BAR], který je velkým příslibem do budoucna. Jedná se o faktor ***někdo koho znáte*** (v originále *somebody you know*). Čtvrtý faktor přirovnávají k tzv. lidské autentizaci, založené na vzájemném poznání. Kdy vám například kolega otevře dveře, protože jste si zapomněli svou přihlašovací kartu. Dveře vám otevřel pouze na základě toho, že vás zná.

Tento proces je nazýván *vouchering*, ve kterém figurují dva druhy aktérů:

- ***Pomocník*** **(*helper*)** - využívá své přihlašovací údaje k pomoci druhému při nouzové autentizaci
- ***Tazatel*** **(*asker*)** – zapomněl své přihlašovací údaje a žádá o pomoc

Pomocník tedy pomocí svých přihlašovacích údajů poskytne tazateli, který svůj token zapomněl, časově omezený přístup, respektive jednorázový přístupový kód (tzv. *vouchcode)*, pomocí kterého se může tazatel autentizovat bez svých přihlašovacích údajů.

2.3.1.1. Autentizační metody

V této části jsou uvedeny nejčastější metody autentizace uživatelů bankovních institucí.

2.3.1.1.5 Jméno a heslo

Použití přihlašovacího jména (případně klientského čísla) v kombinaci s heslem (PIN) patří mezi nejpoužívanější autentizační metody. Hlavním důvodem masivního rozšíření je relativní jednoduchost použití, kdy si uživateli stačí zapamatovat své přihlašovací údaje, které navíc mohou být uživatelsky modifikované, což dále zvyšuje uživatelský komfort.

Bohužel tento fakt je zároveň i největší slabinou tohoto typu autentizace, neboť většina uživatelů si volí velmi jednoduchá hesla, která často souvisejí s jeho osobou (kombinace jména, adresy apod.). Za bezpečná hesla se přitom považují taková hesla, jejichž délka je 8-12 a více znaků, tvořených kombinací písmen, číslic a speciálních znaků. Pokud již uživatel používá relativně silné heslo, často si jej kvůli jeho složitosti zapíše, což představuje velkou hrozbu v případě zcizení.

2.3.1.1.6 Vylepšené heslo

Jedná se o vylepšení předchozí metody tak, aby byla zvýšena odolnost vůči některým typům útoků. Například tím, že nebude přenášeno celé heslo, nebo jen jeho část.

Příkladem vylepšeného hesla může být tzv. *virtual keypad* (virtuální klávesnice), kdy je heslo zadáváno pomocí virtuální klávesnice zobrazené na obrazovce (viz Obrázek 4). To má za výsledek ochranu proti útoku typu keylogging.

Obrázek 4: Ukázka virtuální klávesnice při přihlášení do internet bankingu České spořitelny

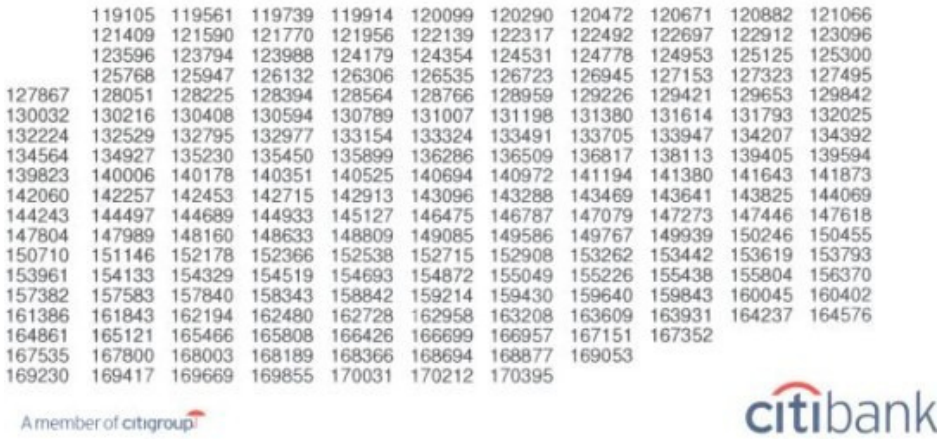
Další metodou vylepšeného hesla je použití tzv. *grid* karty. Uživatelé nejčastěji používají předtištěnou kartu (Obrázek 5) na které jsou ve formě tabulky vytištěny znaky, popřípadě řetězce znaků. Uživatel je poté při autentizaci vyzván k zadání hodnot z určitých sloupců dle vybraných souřadnic.

	A	B	C	D	E	F	G	H	I	J
1	272	189	585	507	077	237	159	363	834	269
2	007	228	246	458	020	183	439	496	907	128
3	846	222	309	985	072	365	316	418	271	003
4	440	983	356	092	144	563	046	936	431	020
5	312	751	658	933	018	051	899	779	895	872
6	336	479	460	529	728	437	386	368	455	450
7	109	939	469	132	586	645	156	558	325	817
8	539	484	337	351	708	422	576	830	110	606
9	501	084	988	176	697	154	163	979	311	666
10	130	901	820	918	932	255	719	731	649	299

Obrázek 5: Ukázka grid karty od společnosti UC software

Velmi podobný principu grid karty je i tzv. *TAN list*. TAN (*Transaction Authentication Number*) znamená autentizační číslo transakce a patří do skupiny jednorázových hesel (podrobností dále). Uživatel má k dispozici seznam TAN a během autentizace se přihlásí svým jménem a heslem a poté je vyzván k zadání ještě nepoužitého TAN ze svého

seznamu (Obrázek 6). Tento použitý TAN si uživatel ve svém seznamu vyškrtne, neboť již jednou použité TAN nebude pro budoucí autentizaci platné.



Obrázek 6: TAN list společnosti Citibank

Pro snížení rizika phishingu (ale ne úplnému zabránění) se používá tzv. *indexed TAN* neboli *iTAN*. Kdy je uživatel vyzván k zadání TAN (nepoužitého) ze svého seznamu, ale s přesně daným indexem. To způsobí, že je daný TAN pevně svázán s danou akcí, a proto útočníkem získaný TAN může být pouze obtížně zneužit.

Mobilní TAN, neboli mTAN, znamená doručení TAN uživateli prostřednictvím jeho mobilního telefonu. Velmi častou se používá k autorizaci transakcí. Tento způsob doručení TAN využívá tzv. *out-of-band* kanál. Ovšem ani tento způsob není zcela oproštěn od zneužití.

Využití grid karet a TAN seznamů lze zařadit do skupiny využívající jednorázové heslo.

2.3.1.1.7 Jednorázové heslo

Jednorázové heslo oproti statickému je při každé prováděné akci jiné. Heslo bývá nejčastěji generováno jednou ze dvou základních metod, časově a čítačově synchronizované. Oba způsoby generování vyžadují speciální zařízení, tzv. token, který v pravidelných časových intervalech generuje jednorázová hesla na základě vnitřního algoritmu (doplněného o čítač, nebo hodiny). Takto vygenerované heslo má omezenou časovou platnost, zpravidla do 1 minuty.

Tokeny můžou být jak hardwarové (Obrázek 7) tak i softwarové, kdy je v klientském systému (chytrém telefonu nebo na PC) uložena aplikace pro generování jednorázového hesla.

Obrázek 7: Ukázka HW tokenu od společnosti RSA pro generování OTP

Pro generování jednorázových hesel mohou být použity běžné platební karty vybavené tzv. *EMV* (*Europay, MasterCard and VISA*) čipem, díky kterému je karta schopna generovat po zadání PIN jednorázové heslo. Tento typ můžeme dále rozdělit na online a offline. Kdy online znamená, že je karta vložena do čtečky, která je přímo spojena s PC, a po zadání PIN na čtečce dojde k zobrazení hesla přímo v PC. OTP heslo je tedy předáno zcela automaticky. Oproti tomu u offline je OTP heslo zobrazeno na displeji čtečky.

2.3.1.1.8 PKI

Při tomto způsobu autentizace se využívá infrastruktury PKI a tedy i certifikátů

Certifikát bývá nejčastěji uložen na přenosném médiu (velmi oblíbený je například USB token), které má za úkol uchránit certifikát proti odcizení (často chráněno PIN).

Zmíněný USB token přináší i další výhody. Například v nich může být striktně a bezpečně oddělená část pro uchování certifikátu/ů a část, která může sloužit jako běžné datové úložiště. Jejich největší předností je ovšem skutečnost, že uživatelé jsou na používání různých USB zařízení zvyklí a tak jim nečiní problém s nimi pracovat.

Dalším médiem pro přenos certifikátů je čipová karta. Tato karta obsahuje kromě certifikátů i další paměť, na kterou si uživatel může uložit další citlivá data. Karta může být kontaktní, tak i bezkontaktní a je chráněna PIN. Uživatel musí pro její použití využít speciální čtečky.

2.3.1.1.9 Biometrika

Použití biometrik v autentizaci není mezi bankovními institucemi příliš rozšířené kvůli vysokým nákladům a u některých metod i neuspokojujícím výsledkům. Jednou z mála výjimek je telefonní bankovnictví.

Z biometrických vlastností se v současné době nejvíce využívá autentizace pomocí hlasu, kdy je klient nejčastěji autentizován odpovědí na otázku operátora (což samo o sobě není moc silná autentizační metoda). Ovšem tato metoda dnes bývá nahrazována automatickým rozpoznáním hlasu. Další využití hlasové autentizace spočívá v zadání aktivačního kódu (nejčastěji čísla), které uživateli nadiktuje operátor.

2.3.1.2. Autentizační metody použité v ČR

U bankovních institucí v České republice jsou k autentizaci uživatelů do internetového bankovnictví nejčastěji používány metody jméno (klientské číslo) a heslo, nebo použití elektronického podpisu (digitálního certifikátu). Tyto metody bývají dále rozšířeny o SMS OTP autentizaci.

V případě mobilního bankovnictví využíváno SIM Toolkitu (popř. Java aplikace) a kombinace jména a hesla.

2.3.2. Další bezpečnostní metody

Z důvodů zajištění vyšší bezpečnosti je nutné kromě zajištění bezpečné autentizace zajistit i zabezpečení akcí prováděných prostřednictvím přímého bankovnictví. Tyto metody spočívají především v detekci podezřelého chování, neobvyklých transakcí apod.

2.3.2.1. Vrstvená bezpečnost

V roce 2011 vydala společnost FFIEC aktualizovanou *Supplement to Authentication in an Internet Banking*. Ve které mimo jiné poukazuje na skutečnost, že každá sebesilnější autentizační metoda může být kompromitována a budoucnost představuje použití vrstvené bezpečnosti, která využívá komplexního bezpečnostního řešení skládajícího se z několika samostatných bezpečnostních prvků.

Vrstvená bezpečnost se vyznačuje použitím různých kontrol na různých místech transakčního procesu, takže slabina jedné kontroly je kompenzována silou jiné kontroly. Vrstvená bezpečnost může podstatně zvýšit bezpečnost internetových služeb, být účinná při ochraně citlivých uživatelských dat, předcházet krádežím identity, snížení zcizení účtů a z toho plynoucí finanční ztráty [FFIEC1].

Vrstvené bezpečnostní programy by měly obsahovat následující kontroly [FFIEC1]:

- Detekce podezřelých transakcí a monitorovací systémy
- duální uživatelská autorizace použitím rozdílných autorizačních zařízení
- out-of band autorizace (autorizace pomocí jiného kanálu)
- nastavení transakčních limitů
- rozšířená kontrola nad aktivitami v účtu
- blacklist IP adres serverů podezřelých z podvodných aktivit
- postupy a politiky pro identifikaci klientských zařízení, které jsou identifikovány jako potenciálně kompromitované
- vzdělávání zákazníků

Některé z těchto uvedených metod již byly popsány. Další, které představují moderní bezpečnostní metody, budou popsány dále.

2.3.2.2. Ochrana proti krádeži identity

V současnosti některé bankovní instituce zavádějí novou službu pro zákazníky v podobě ochrany proti krádeži identity. Tato ochrana spočívá v zajištění monitoringu a ochraně klientských dat, pravidelné zasílání reportů o klientských účtech, zasílání upozornění v případě nenadálých událostí a zajištění dodatečné asistence.

Existuje i mnoho soukromých firem zabývajících se problematikou krádeže identity. Některé z nich ovšem využívají strachu zákazníků a jimi nabízené služby poskytují pouze falešný pocit bezpečí.

Příkladem může být služba „Informování o výskytu Vašich citlivých údajů na internetových stránkách“. V tomto případě bude uživatel pouze **informován** o výskytu

svých údajů na často nebezpečných stránkách, nebo na internetovém černém trhu, ale už nenabízejí žádnou možnost, jak takto zveřejněná data z těchto stránek **odstranit**.

2.3.2.3. Systémy pro detekci podvodného chování

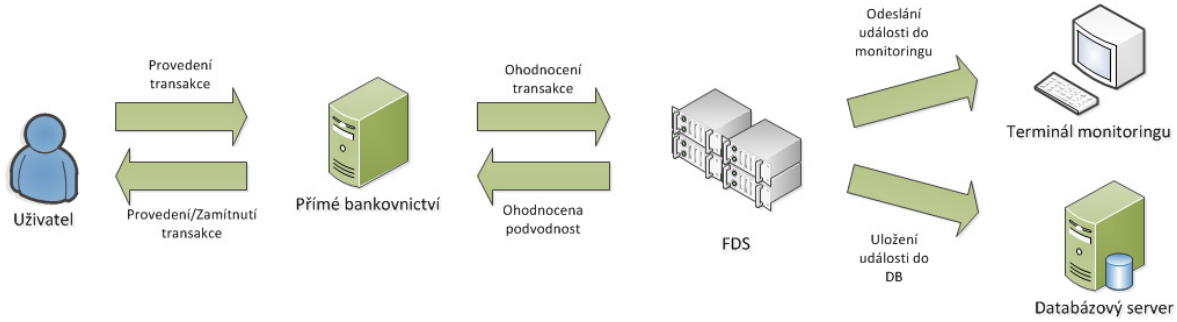
Systémy pro detekci podvodného, podezřelého nebo abnormálního chování, které v reálném čase monitorují transakce, se nazývají *Fraud Detecion Systems* (zkráceně FDS).

Tyto systémy využívají pro analýzu používaných dat a rozpoznání podvodných transakcí předdefinovaných pravidel a někdy i metod umělé inteligence. Pravidla zahrnují mimo jiné ověření oproti blacklistům, překročení limitů či počtu pokusů o přihlášení. Systémy se ovšem nemusejí jen zabývat daty, s kterými je transakce svázána, ale i samotným chováním uživatele (detailněji popsáno dále).

Výsledkem vyhodnocení FDS může být několik, od automatizovaného zamítnutí operace, po telefonický kontakt uživatele pro ověření operace.

FDS mají samozřejmě mnohem širší využití než jen u bankovních institucí. Pro zajímavost například česká společnost Mycromind nabízí systém FFDS, neboli Fuel FDS, která v reálném čase analyzuje transakce na čerpacích stanicích (čerpání, doplňování, platba atd.).

Ukázku použití FDS v přímém bankovnictví zobrazuje Obrázek 8: Ukázka použití FDS v přímém bankovnictví.



Obrázek 8: Ukázka použití FDS v přímém bankovnictví

2.3.2.4. Detekce anomálií

Protože všechny útoky na přímé bankovnictví mají jeden společný element – při jakémkoli útoku musí existovat interakce s internetovým (příp. jiným) bankovnictvím a právě v tomto bodě mají bankovní instituce nejvyšší šanci proti útokům zasáhnout – použitím detekce anomálií.

Detekce anomálií spočívá v detekci akcí, které se nějakým způsobem odlišují od normy (např. počet transakcí za den, odeslání nezvykle velké částky). V současné době detektory anomálií vychází především z historických záznamů chování uživatele, jakou jsou například obvyklá IP adresa, čas přihlášení apod. (ovšem ty mohou být také kompromitovány). Na základě těchto poznatků jsou poté stanovena pravidla, jejichž úkolem je reagovat na výskyt určité anomálie.

Velkým problémem však bývá právě stanovení těchto pravidel, často specifických pro jednotlivé uživatele, nebo skupiny uživatelů. Špatně nastavená pravidla totiž způsobují generování falešných událostí, které zapříčiňují zamítnutí (v literatuře udáváno jako *FFR - false rejection rate*), nebo naopak nezachycení podezřelé události (*FAR - false acceptation rate*). Tyto události poté zahlcují jak systém (případně operátory monitoringu), tak i uživatele.

V oblasti detekce proto stále přicházejí nové a sofistikovanější detekce anomálií. Jednou z nich, které se přikládá velká budoucnost, je detekce anomálií zvaná **behaviorální biometrika**.

2.3.2.5. Behaviorální biometrika

Behaviorální biometrika, neboli biometrika chování uživatele, oproti tradiční detekci anomálií, ve kterých je obvykle vycházeno z předchozích zkušeností s chováním uživatele (například uživatel vždy po přihlášení do přímého bankovnictví nejprve zkontroluje stav účtu, poté se podívá na elektronický výpis a tak dále), využívá biometrického chování uživatelů v prostředí přímého bankovnictví.

Existuje velké množství technik pro metodu behaviorální biometriky, mimo jiné jsou to například:

- **ECG** - techniky zaměřené na elektromagnetické signály srdce
- **EEG -** techniky zaměřené na elektromagnetické signály mozku
- **Chůze** – styl chůze
- **Dynamika psaní** – může být pouze sledována dynamika psaní, nebo na specializovaných klávesnicích tlak stisku
- **Styl psaní**

- **Hlas**

Samozřejmě, že ne všechny tyto techniky jsou použitelné v komerční praxi. Zejména kvůli své složitosti a finanční náročnosti (potřeba nejrůznějších hardwarových prvků) a v neposlední řadě i uživatelské přívětivosti. Ovšem například dynamika psaní patří mezi nejlépe hodnocené metody a její použití je již zavedeno v praxi (např. Unicredit bank).

Dynamika psaní pro svou funkcionalitu používá statistických údajů, nebo neuronových map, kdy jsou posuzovány jednotlivé aspekty psaní (síla stisku, prodleva mezi stisky atd.). Na základě těchto údajů se dá velmi přesně určit identita uživatele, protože lze snadno rozpoznat rozdíl mezi uživatelem, který dokáže napsat 30 slov za minutu a uživatelem, který jich zvládne 70. Stejně tak lze snadno pomocí dynamiky psaní rozpoznat praváka od leváka.

Při každé autentizaci uživatele, kdy uživatel zadává ověřovací řetězec, je tento porovnáván s předešlými záznamy, a v případě úspěšné autentizace je uložen mezi záznamy pro budoucí použití.

Oproti ostatním behaviorálním technikám vyniká metoda dynamiky psaní absencí potřeby externího zařízení (kromě případů sledujících sílu stisku, kdy je potřeba speciální klávesnice) a s ní související uživatelskou přívětivostí (oproti například otiskům prstů). Navíc ji lze v principu použít i v mobilním bankovnictví.

Další velmi používanou metodou behaviorální biometriky je rozpoznání hlasu. Bylo prokázáno, že ani nejlepší imitátoři nedokáží napodobit lidský hlas, který je pro každého jedince specifický. Pokud útočník získá nahrávku hlasu uživatele a bude ji chtít použít, systém to velice snadno pozná, neboť nahrávka se bude stoprocentně schodovat s porovnávaným záznamem a je tudíž jasné, že nahrávka byla podvržena, protože žádný člověk nedovede danou frázi vyslovit pokaždé stejně.

K rozpoznání hlasu, nebo spíše verifikaci uživatele dle jeho hlasu, slouží krátká nahrávka, někdy označovaná jako tzv. *voiceprint,* který je uložen v systému nazývaném *enrollment*.

Systémy pro identifikaci uživatele na základě hlasu můžeme klasifikovat na:

- **text dependent** – uživatel je vyzván aby vyslovil frázi, kterou mu systém přehrál, nebo aby přečetl zobrazenou frázi
- **text independent** – uživatel může vyslovit cokoli a jeho hlas je vyhodnocován v průběhu

Samozřejmě i tato metoda má své úskalí. Například v případě nemoci uživatele, kdy nebude schopen přesně interpretovat frázi. Také útok, kdy se útočník bude vydávat za poskytovatele služby, je velmi nebezpečný, neboť uživatel jen velmi těžko ověří zda se opravdu jedná o pravého poskytovatele (lze realizovat například nahráním nějaké uvítací fráze, aby uživatel poznal, zda opravdu komunikuje s pravým poskytovatelem).

2.3.2.6. Risk based authentication

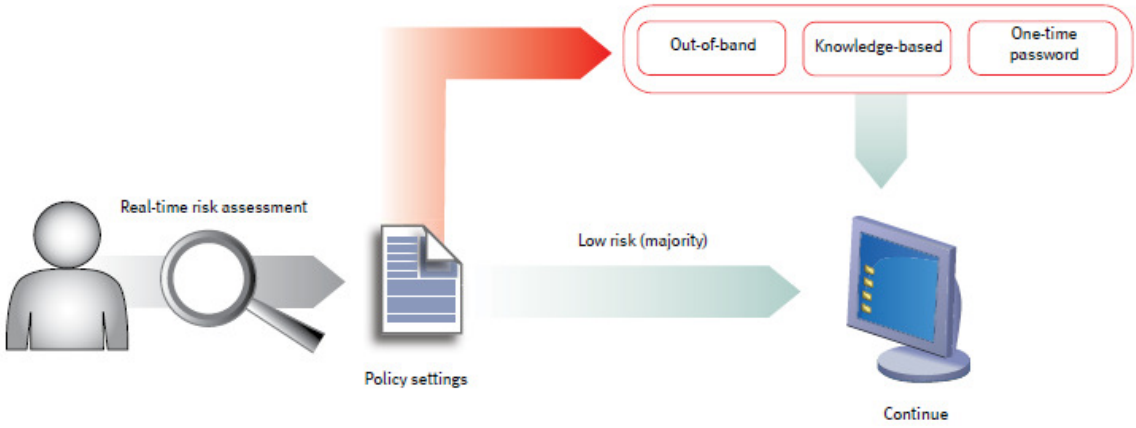
Autentizace založená na rizikovosti neboli adaptivní autentizace, tvoří nedílnou součást moderních FDS systémů. Hlavním principem je výpočet tzv. *risk score* (faktor rizikovosti), dle tohoto faktoru a dalších parametrů (vnitřní politiky bankovní instituce, scénáře chování) je dále rozhodnuto, zda bude vyžadována další, sekundární, autentizace (to v případě, že faktor rizikovosti ohodnotí autentizaci jako potenciálně nebezpečnou), nebo bude uživatel autentizován klasickou cestou. Sekundární autentizací většinou bývá nějaký druh out-of-band autentizace (SMS, email) nebo zodpovězení otázky metodou challenge-request.

Výpočet faktoru rizikovosti probíhá v reálném čase a spočívá ve vyhodnocení mnoha informací. Mezi tyto informace patří:

- Informace o uživatelském zařízení
- Připojení k internetu (IP, proxy, poloha)
- Časová hlediska (obvyklé dny, určité hodiny, frekvence)
- Historické aspekty (průměrné pohyby na účtu)
- Předdefinované faktory (blacklisty čísel účtů, lokalit aj.)

Příkladem systému založenému na adaptivní autentizaci může být systém *RSA AA* (*Adaptive Authentization*), od stejnojmenné společnosti, který mimo jiné obsahuje i

automatickou obranu proti útoku typu phishing, kdy je uživateli zobrazen jeho osobní obrázek, a to má za následek, že uživatel okamžitě pozná, zda se jedná o podvodnou stránku. Na obrázku níže (Obrázek 9: Zjednodušené schéma Risk-based autentizačního systému [RSA]) vidíte schéma RSA AA systému.



Obrázek 9: Zjednodušené schéma Risk-based autentizačního systému [RSA]

Tento způsob autentizace s sebou přináší velkou výhodu zejména ve vyšší uživatelské přívětivosti, neboť běžný uživatel ve většině případů nebude obtěžován dalšími bezpečnostními prvky a zároveň se zvýší celková bezpečnost autentizačního mechanismu.

3. Praktická část

3.1. Analýza autentizačních metod

Pro každou z metod uvedených v kapitole 2.3.1.1 existuje modifikace pro určitý kanál přímého bankovnictví a zároveň každá z nich disponuje specifickými vlastnostmi, jejichž vyhodnocení je úkolem této analýzy.

3.1.1. Metodika

Pro hodnocení metod byly stanoveny následující metriky, které zahrnují parametry, důležité pro výběr nejvhodnější autentizační metody:

- **Síla autentizace (SA)**
- **Uživatelská přívětivost (UP)**
- **Celkové náklady (TCO)**
- **Další aspekty (DA)**

Jednotlivé metriky v sobě zahrnují určitá dílčí kritéria, která se podílejí na celkovém hodnocení dané metriky. Tato kritéria jsou vždy ohodnocena na stupnici od 1 (nejhorší) do 5 (nejlepší) a každému z nich je přiřazen určitý váhový koeficient, který odráží jejich význam pro celkové hodnocení. Váhový koeficient musí být pro každou metriku vždy v součtu roven 10, nezávisle na počtu jednotlivých kritérií metriky.

Tabulka metrik s jejich kritérii je zobrazena v příloze 72. Kompletní tabulku kritérií s jejich ohodnocením, ze kterého bylo v následujícím textu vycházeno, naleznete v příloze 7.1.

Pro analýzu jsem vybral takový výčet autentizačních metod, aby zahrnoval co nejširší spektrum používaných autentizačních metod. Výčet tedy zahrnuje jak klasické autentizační metody, tak i nové, nepříliš rozšířené metody.

Výčet vybraných autentizačních metod :

1. Jméno, heslo, klasická klávesnice
2. Jméno, heslo , virtuální klávesnice
3. Jméno, heslo + SMS

4. Autentizace ověřovacími otázkami
5. SIM Toolkit
6. Grid karty
7. OTP token a heslo
8. OTP token s klávesnici a displejem + heslo
9. OTP token,čtečka s klávesnici a displejem + heslo
10. USB token
11. Čipová karta a čtečka
12. Kvalifikovaný PKI certifikát
13. Otisk prstu a PIN
14. Rozpoznání hlasu a PIN
15. Dynamika psaní a PIN

Výsledky analýzy jsou zobrazeny kromě číselných hodnot ve formě tabulky i pomocí grafu, jež představuje poměr hodnot metody vůči celkovým průměrným hodnotám přes všechny hodnocené metody.

Graf má hvězdicový tvar, kdy jednotlivé osy značí metriky (v grafu znázorněny jako zkratky těchto metrik, tj. síla autentizace = SA, Uživatelská přívětivost = UP, Celkové náklady = TCO, Další aspekty = DA). Pro lepší přehlednost grafu byly získané hodnoty normalizovány v poměru k maximu z dané metriky.

3.1.2. Jméno, heslo a klasická klávesnice

Popis metody: Autentizace zadáním přihlašovacího jména a hesla pomocí klasické hardwarové klávesnice.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
1,00	4,60	5,00	3,90

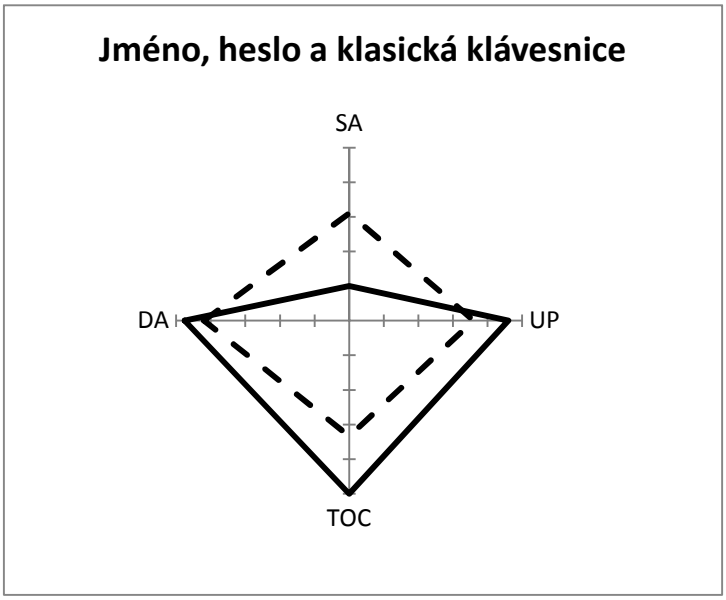
Tabulka 2: Vyhodnocení metody Jméno,heslo a klasická klávesnice

Síla autentizace: Velmi nízká. Heslo lze velmi snadno zcizit a zneužít. Perspektiva metody z tohoto důvodu také na velmi nízké úrovni.

Uživatelská přívětivost: Vysoká. Heslo je pro uživatele lehce zapamatovatelné, lze ho modifikovat dle požadavků zákazníka. Autentizační proces je pro uživatele triviální.

TOC: Nejnižší možné TCO. Náklady na implementaci a provoz metody jsou minimální.

Další aspekty: Nízké požadavky na infrastrukturu. Nezávislost na třetích stranách. Rychlé nasazení. Horší životnost metody.



Obrázek 10: Vyhodnocení metody Jméno,heslo, klasická klávesnice oproti průměrným výsledkům

Shrnutí: Autentizace použitím klasického spojení jména a hesla je pro uživatele velmi komfortní a intuitivní. Stejně tak náklady na provoz a implementaci jsou nízké. Oproti tomu autentizační síla je na velmi malé úrovni a to se odráží i do životnosti metody.

3.1.3. Jméno, heslo a virtuální klávesnice

Popis metody: Autentizace zadáním jména a hesla pomocí virtuální klávesnice zobrazené na obrazovce.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
1,30	4,10	5,00	3,90

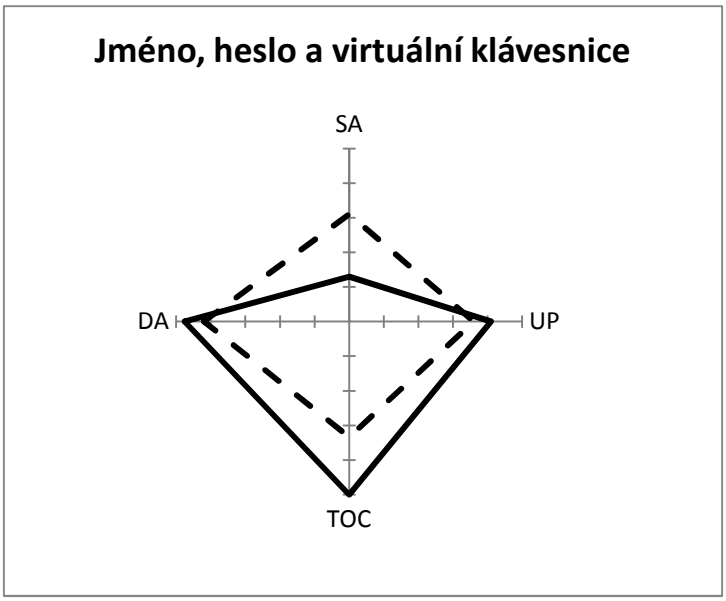
Tabulka 3: Vyhodnocení metody Jméno, heslo a virtuální klávesnice

Síla autentizace: Velmi nízká. Vysoká hrozba odcizení hesla.

Uživatelská přívětivost: Nadprůměrná. Uživatelé pouze nepoužijí klasickou klávesnici, může to být trochu zdlouhavější. Finanční nároky na uživatele nulové.

TOC: Nejnižší možné TCO. Náklady na implementaci a provoz metody jsou minimální.

Další aspekty: Nízké požadavky na infrastrukturu. Nezávislost na třetích stranách. Rychlé nasazení. Horší životnost metody.



Obrázek 11: Vyhodnocení metody Jméno,heslo, virtuální klávesnice oproti průměrným výsledkům

Shrnutí: Stejně jako u předchozí metody získává dobré ohodnocení z hlediska nákladů, nezávislosti na třetích stranách a dobré uživatelské přívětivosti. Metoda má větší autentizační sílu oproti předchozí, avšak stále velmi podprůměrnou.

3.1.4. Jméno, heslo a SMS

Popis metody: Autentizace zadáním jména, hesla doplněná jednorázovým autentizačním kódem získaným formou autentizační SMS.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
3,60	**3,15**	**1,80**	**3,50**

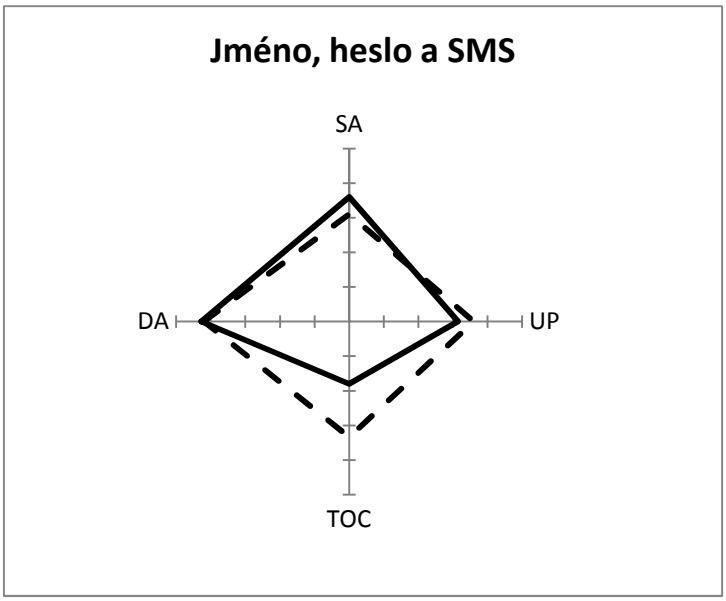
Tabulka 4: Vyhodnocení metody Jméno, heslo a SMS

Síla autentizace: Lehce nadprůměrná. Důvodem je použití SMS jako druhého autentizačního faktoru. Perspektiva patří mezi průměrné.

Uživatelská přívětivost: Nutnost přepsání jednorázového hesla z SMS zprávy může činit problémy některým uživatelům.

TOC: Nákladný provoz z důvodu zasílání SMS, smlouvy s operátory.

Další aspekty: Nutnost třetích stran – mobilních operátorů. Pokrytí GSM sítě.



Obrázek 12: : Vyhodnocení metody Jméno,heslo a SMS oproti průměrným výsledkům

Shrnutí: Metoda je díky použití druhého kanálu v oblasti síly autentizace mírně nadprůměrná. V ostatních oblastech patří k průměrným, avšak v případě TOC lze spatřit velký vliv nákladů pro bankovní instituce, které jsou spojené se zasíláním SMS zpráv.

3.1.5. Autentizace ověřovacími otázkami

Popis metody: Autentizace během telefonního hovoru uživatele s operátorem, kdy operátor autentizuje uživatele pokládáním předem definovaných dotazů, jako jsou například datum narození apod.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
1,00	**4,00**	**3,40**	**3,20**

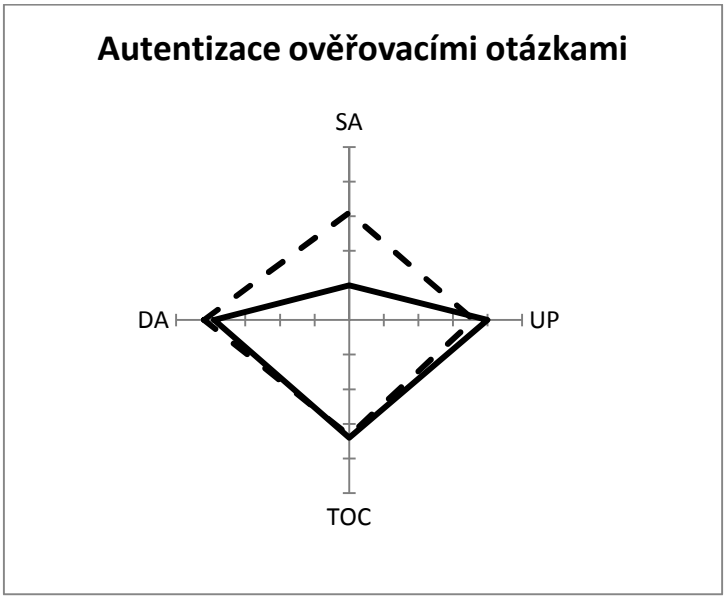
Tabulka 5: Vyhodnocení metody Autentizace ověřovacími otázkami

Síla autentizace: Velmi nízká. Operátor nemá zaručeno, že hovoří s oprávněnou osobou kvůli možné krádeži identifikačních údajů.

Uživatelská přívětivost: Komfort uživatele snižován pokládáním otázek. Velmi vysoká mobilita metody. Nízká finanční náročnost pro uživatele.

TOC: Náklady jsou kvůli potřebě většího množství operátorů vyšší.

Další aspekty: Velmi nízká životnost metody z důvodu nízké úrovně síly autentizace.



Obrázek 13: Vyhodnocení metody Autentizace ověřovacími otázkami oproti průměrným výsledkům

Shrnutí: Autentizace ověřovacími otázkami je z hlediska síly autentizace velmi slabá, což snižuje i její životnost. Důvodem je fakt, že operátor si nikdy nemůže být jist, zda opravdu hovoří s konkrétním uživatelem.

3.1.6. SIM Toolkit

Popis metody: Speciální SIM karta v telefonu uživatele, umožňující přístup k mobilnímu bankovnictví formou předdefinovaných a šifrovaných SMS zpráv.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
3,00	**4,00**	**3,60**	**3,45**

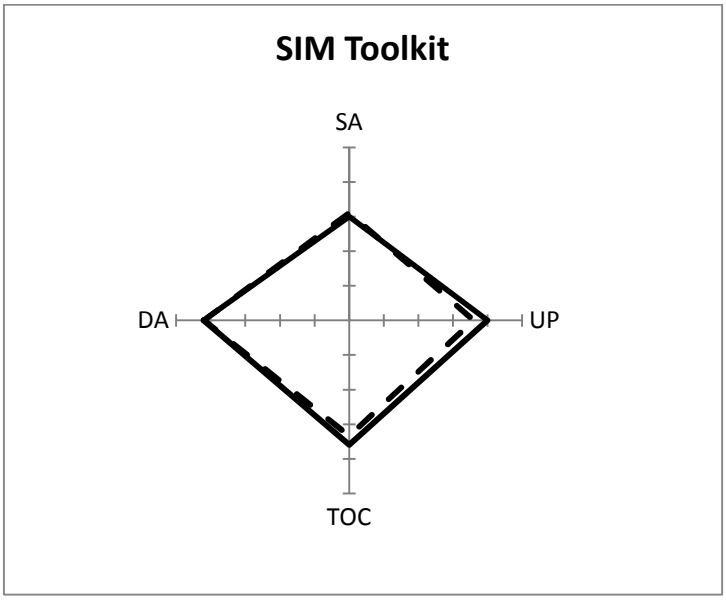
Tabulka 6: Vyhodnocení metody SIM Toolkit

Síla autentizace: Průměrná bezpečnost. Šifrované spojení.

Uživatelská přívětivost: Jednoduchost použití mobilní aplikace. Nutnost osobně vyzvednout SIM kartu snižuje hodnocení.

TOC: Vyšší náklady na vydávání SIM karet a provoz metody.

Další aspekty: Závislost na třetích stranách – výrobci SIM karet. Nákladná distribuce.



Obrázek 14: Vyhodnocení metody SIM Toolkit oproti průměrným výsledkům

Shrnutí: Tato autentizační metoda dosahuje průměrných výsledků ve všech zkoumaných oblastech. Vyšší náklady na distribuci a provoz vyvažuje vyšší autentizační síla.

3.1.7. Grid karty

Popis metody: Autentizace uživatelským jménem a heslem doplněná o jednorázové heslo z grid karty, které uživatel zadá dle určených souřadnic.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
2,20	**2,45**	**3,00**	**3,00**

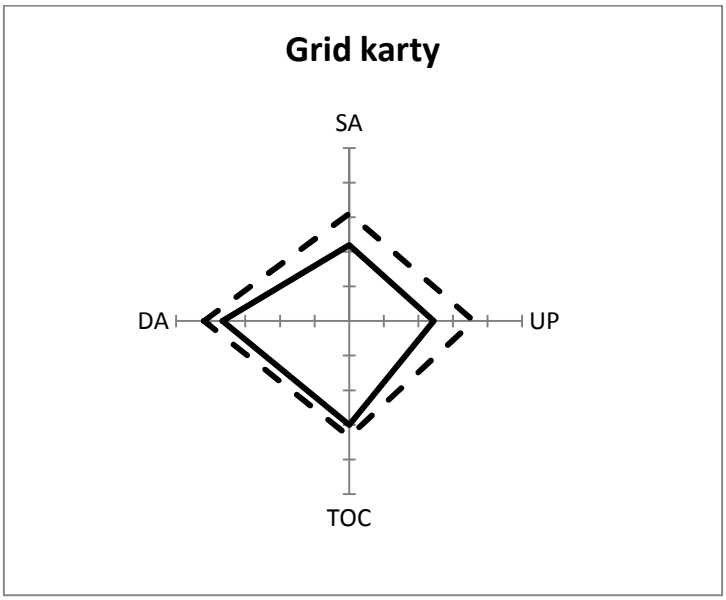
Tabulka 7: Vyhodnocení metody Grid karty

Síla autentizace: Nízká. Lze jednoduše zcizit zadávané údaje.

Uživatelská přívětivost: Nízká. Uživatel je nucen hledat příslušné jednorázové heslo a správně ho přepsat. Nutnost osobního vyzvednutí grid karet.

TOC: Průměrné. Náklady na opětovné vydání grid karet.

Další aspekty: Malá životnost metody. Nákladná distribuce.



Obrázek 15: Vyhodnocení metody Grid karty oproti průměrným výsledkům

Shrnutí: Z pohledu všech hledisek je tato metoda velmi podprůměrná. Použití grid karet sice zvyšuje sílu autentizace, ale stále se jedná o pouze jednofaktorovou autentizaci, která nedokáže zabránit odcizení údajů. Uživatelská přívětivost je také na nízké úrovni, kvůli přepisování netriviálního kódu dle vybraných souřadnic.

3.1.8. OTP token a heslo

Popis metody: Uživatel má k dispozici OTP token generující v pravidelných intervalech jednorázové heslo, které uživatel využije k autentizace ve spojení se svým heslem.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
3,40	**3,80**	**3,60**	**3,50**

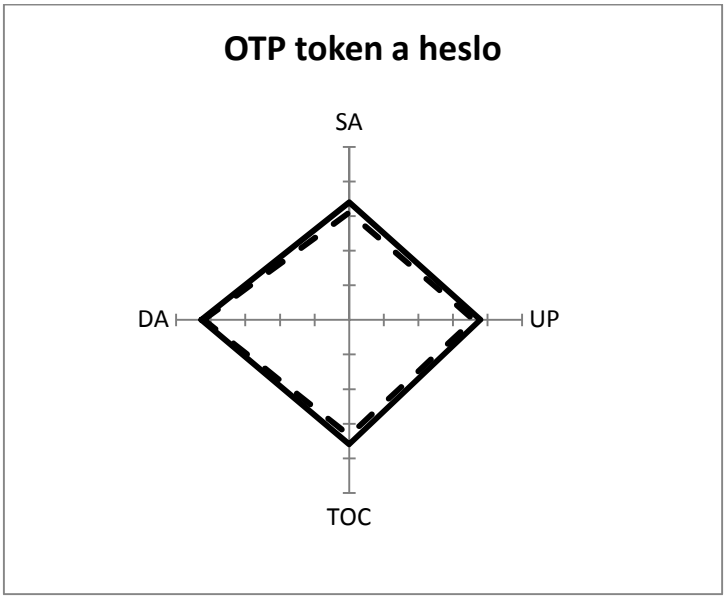
Tabulka 8: Vyhodnocení metody OTP token a heslo

Síla autentizace: Vysoká. Díky použití jednorázového hesla, jehož platnost je časově omezena.

Uživatelská přívětivost: Lehce nadprůměrná. Uživatel jednoduše přepíše jednorázové heslo. Nutnost mít token stále u sebe.

TOC: Náklady na implementaci jsou průměrné. Provoz vyžaduje málo frekventované (v řádech let) obměny zařízení.

Další aspekty: Průměrná závislost na třetích stranách. Vyšší náklady na distribuci. Dlouhá životnost.



Obrázek 16: Vyhodnocení metody OTP token a heslo oproti průměrným výsledkům

Shrnutí: Oproti předchozí metodě nabízí díky použití časově omezeného jednorázového hesla i s ohledem na perspektivu metody vyšší autentizační sílu. Za hlavní nevýhodu lze označit finanční náročnost na distribuci a provoz tokenů.

3.1.9. OTP token s klávesnicí a displejem, heslo

Popis metody: OTP token je doplněn o klávesnici, určenou pro zadání hesla na základě kterého je poté vygenerováno jednorázové heslo. Toto heslo je poté použito k samotné autentizaci pro doplnění klasického hesla.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
5,00	**3,90**	**3,60**	**3,40**

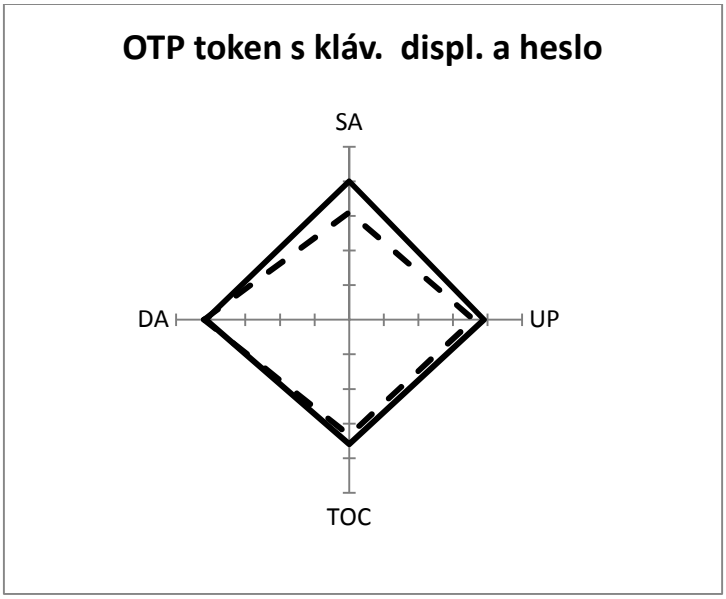
Tabulka 9: Vyhodnocení metody OTP token s klávesnicí a displejem

Síla autentizace: Úroveň zabezpečení je vysoká, stejně tak i perspektiva metody.

Uživatelská přívětivost: Snížena o nutnost zadání hesla před generováním jednorázového hesla. Velkým kladem je zde mobilita metody.

TOC: Náklady na provoz a implementaci patří k průměrným. Nutno počítat s výměnou zařízení v delším časovém horizontu.

Další aspekty: Závislost na třetích stranách a náročnost podpory a distribuce snižuje hodnocení v této oblasti.



Obrázek 17: Vyhodnocení metody OTP token s klávesnicí a displejem, heslo oproti průměrným výsledkům

Shrnutí: Poskytuje stejné výsledky jako metoda OTP tokenu a hesla, avšak díky klávesnici dosahuje lepší úrovně zabezpečení, které ovšem na druhou stranu způsobuje mírné snížení uživatelské přívětivosti.

3.1.10. OTP token, čtečka s klávesnicí a displejem, heslo

Popis metody: Uživatel zasune token do čtečky a zadá heslo. Čtečka poté zobrazí jednorázové heslo, které uživatel použije ve spojení s obyčejným heslem k autentizaci.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
4,30	2,00	3,00	3,20

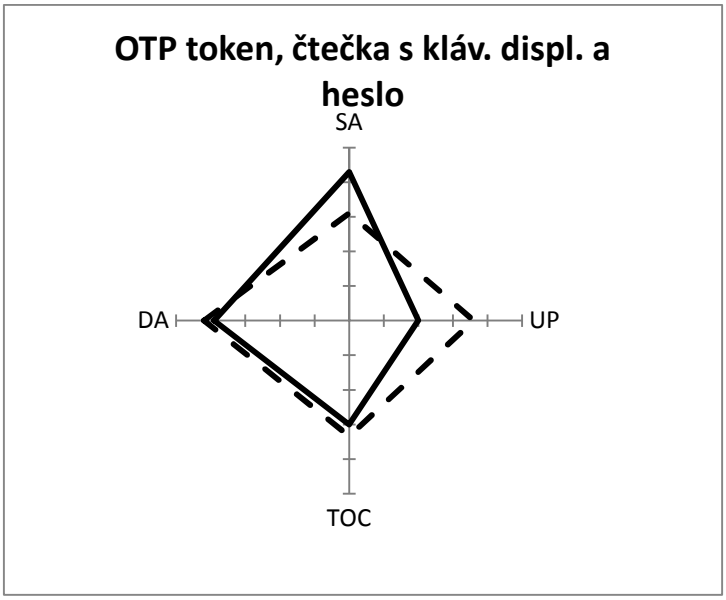
Tabulka 10: Vyhodnocení metody OTP token, čtečka s klávesnicí a displejem, heslo

Síla autentizace: Úroveň zabezpečení je vysoká, stejně tak i perspektiva metody.

Uživatelská přívětivost: Podprůměrná z důvodu nutnosti použití čtečky. Klesá také mobilita metody a nezanedbatelné jsou i finanční nároky pro uživatele.

TOC: Vyšší náklady na implementaci a provoz metody.

Další aspekty: Vyšší nároky na podporu uživatelům. Finančně náročná distribuce zařízení.



Obrázek 18: Vyhodnocení metody OTP token,čtečka, klávesnice, displej, heslo oproti průměrným výsledkům

Shrnutí: Použití čtečky zvyšuje celkovou úroveň zabezpečení, ale zároveň způsobuje nižší uživatelskou přívětivost. Náklady na tuto metodu

jsou podprůměrné zejména kvůli distribuci a podpoře zákaznických zařízení.

3.1.11. USB token

Popis metody: Uživatel se autentizuje pomocí certifikátu uloženým v šifrované podobě na USB tokenu.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
4,60	2,90	3,00	3,70

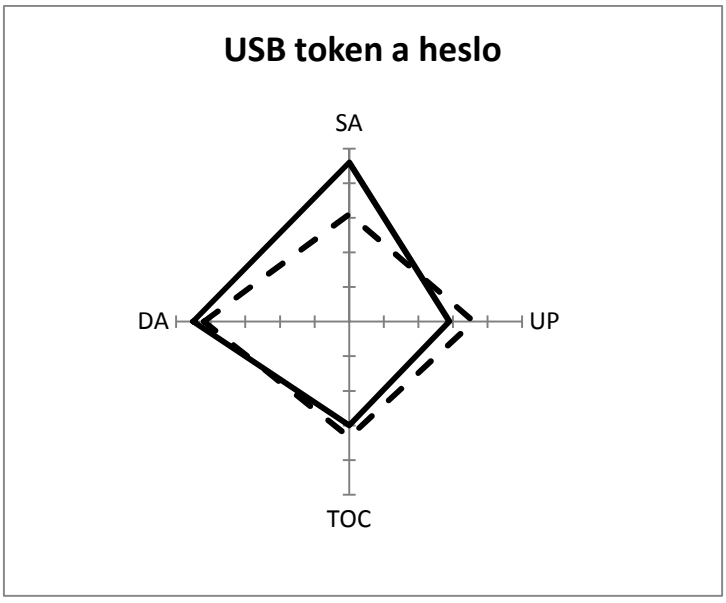
Tabulka 11: Vyhodnocení metody USB token

Síla autentizace: Z důvodu použití certifikátu velmi vysoká úroveň zabezpečení.

Uživatelská přívětivost: Vyšší finanční nároky na uživatele a průměrný komfort kompenzuje vysoká mobilita metody.

TOC: Finanční náročnost implementace a provozu se vyskytuje v průměrných hodnotách.

Další aspekty: Nutná podpora při problémech v práci s certifikátem.



Obrázek 19: Vyhodnocení metody USB token oproti průměrným výsledkům

Shrnutí: Metoda USB tokenu nabízí z hlediska autentizační síly vhodnou metodu. Vyšší náklady a nižší uživatelská přívětivost znehodnocují perspektivu této metody.

3.1.12. Čipová karta a čtečka

Popis metody: Certifikát uložený na kartě je pomocí čtečky načten do počítače a použit pro autentizaci uživatele.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
4,60	**3,10**	**3,00**	**3,55**

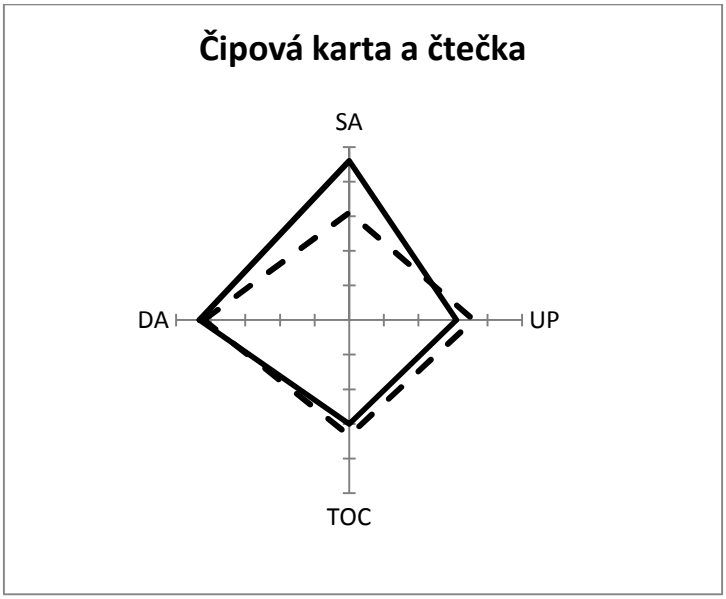
Tabulka 12: Vyhodnocení metody Čipová karta a čtečka

Síla autentizace: Velmi vysoká úroveň zabezpečení a vysoká perspektiva metody způsobují maximální úroveň síly autentizace.

Uživatelská přívětivost: Použití čtečky snižuje komfort, jednoduchost použití a mobilitu metody.

TOC: Náklady se rovnají průměrným hodnotám.

Další aspekty: Distribuce karet, podpora a závislost na třetích stranách snižují hodnocení v této oblasti pod průměrné hodnoty.



Obrázek 20: Vyhodnocení metody Čipová karta a čtečka klávesnice oproti průměrným výsledkům

Shrnutí: Vysoká úroveň zabezpečení je znehodnocena silně podprůměrnou uživatelskou přívětivostí způsobenou použitím čtečky, zvýšeném finančním podílu uživatele a v neposlední řadě také nízkou mobilitou.

3.1.13. Kvalifikovaný PKI certifikát

Popis metody: Uživatel se autentizuje použitím kvalifikovaného certifikátu, který je uložen na pevném disku.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
3,00	3,50	2,80	4,10

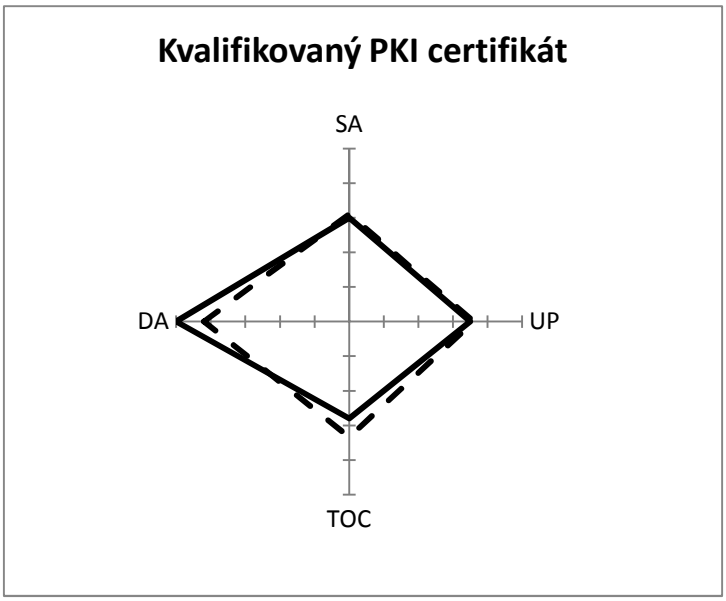
Tabulka 13: Vyhodnocení metody Kvalifikovaná PKI certifikát

Síla autentizace: Autentizace použitím kvalifikovaného certifikátu představuje nejsilnější formu autentizace avšak uložení certifikátu na pevném disku velmi snižuje hodnocení.

Uživatelská přívětivost: Velmi nízká mobilita, horší sociální přijatelnost a průměrný uživatelský komfort způsobují nízké hodnocení v této oblasti.

TOC: Náklady na provoz PKI infrastruktury jsou velmi vysoké.

Další aspekty: Nejvyšším záporem metody je nutná podpora uživatelů při práci s certifikáty a úprava infrastruktury pro použití PKI.



Obrázek 21: Vyhodnocení metody Kvalifikovaný PKI certifikát oproti průměrným výsledkům

Shrnutí: Vysoká úroveň zabezpečení z pohledu certifikátu je výrazně znehodnocena uložením certifikátu na disku, který tak není nijak chráněn proti zneužití. Zároveň mobilita je z tohoto důvodu také na nízké úrovni. Tato fakta tak sráží výhody PKI infrastruktury.

3.1.14. Otisk prstu a PIN

Popis metody: Uživatel se autentizuje sejmutím otisku prstu na k tomu určeném zařízení a doplněním PIN kódu.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
5,00	**2,80**	**2,00**	**3,10**

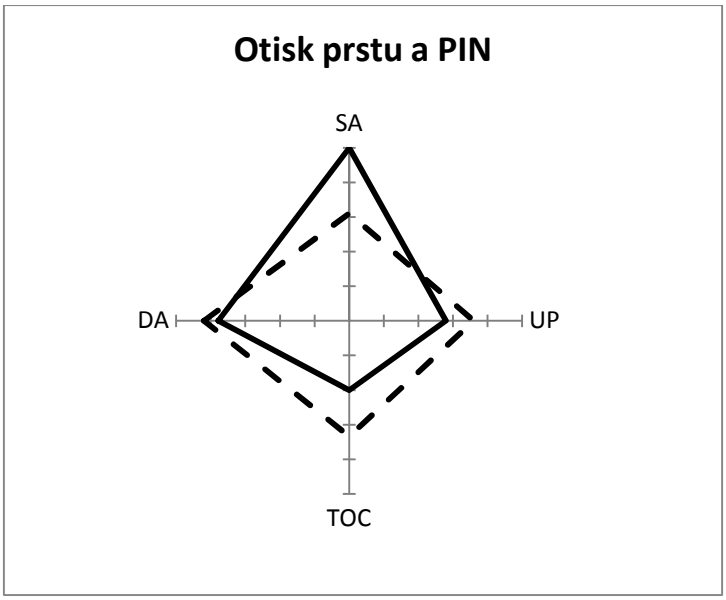
Tabulka 14: Vyhodnocení metody Otisk prstu a PIN

Síla autentizace: Otisk prstu je originálním a těžko odcizitelným biometrickým faktorem doplněným o další faktor v podobě PIN.

Uživatelská přívětivost: Použití čtečky otisků prstů je netriviální, místy je nutné snímání opakovat. Mobilita a nutnost pořízení snímacího zařizují snižují hodnocení v této oblasti.

TOC: Implementační náklady jsou velmi vysoké z důvodu použití sofistikovaného software a hardware pro práci s otisky prstů s tímto faktem je spojena i vysoká cena provozu.

Další aspekty: Závislost na třetích stranách je v případě této metody velmi vysoká. Ostatní parametry paří k průměrným.



Obrázek 22: Vyhodnocení metody Otisk prstu a PIN oproti průměrným výsledkům

Shrnutí: Náklady na provoz a implementaci, závislost na třetích stranách a nulová mobilita snižují možnosti použití této metody i přes její velmi vysokou úroveň zabezpečení.

3.1.15. Rozpoznání hlasu a PIN

Popis metody: Uživatel je po klasickém přihlášení jménem a PIN vyzván k vyslovení určité fráze, nebo libovolného textu, pomocí kterého je jednoznačně identifikován a autentizován do systému.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
3,00	**5,00**	**3,60**	**2,80**

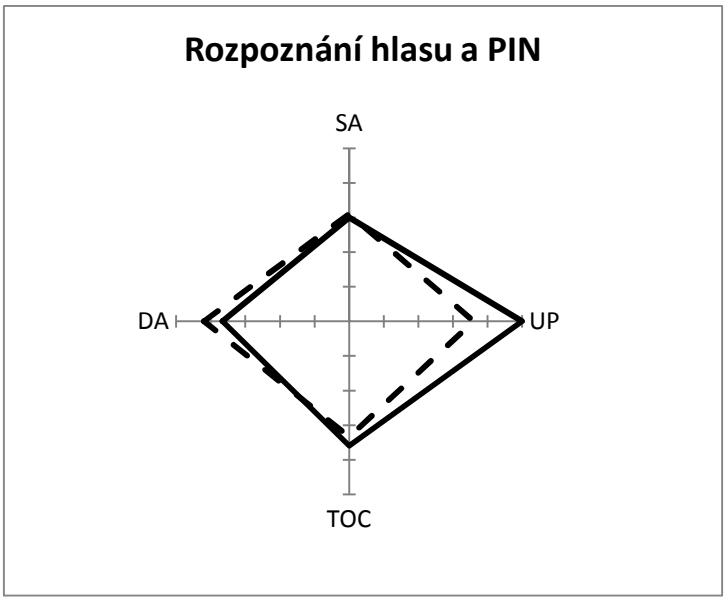
Tabulka 15: Vyhodnocení metody Rozpoznání hlasu a PIN

Síla autentizace: Použití metody rozpoznání hlasu jako druhý faktor naráží na legislativní překážky, ale i na nedokonalost metody, kdy dochází k nesprávné identifikaci uživatele.

Uživatelská přívětivost: Autentizace použití této metody je zcela triviální, pro uživatele nenáročná a finanční náročnost nulová.

TOC: Náklady na implementaci jsou průměrné.

Další aspekty: Velmi negativním jevem je závislost na třetích stranách. Životnost a požadavky na infrastrukturu jsou na průměrné úrovni.



Obrázek 23: Vyhodnocení metody Rozpoznání hlasu a PIN oproti průměrným výsledkům

Shrnutí: Metoda Rozpoznání hlasu a PIN poskytuje vysoký uživatelský komfort, ale z důvodů nedokonalých rozpoznávacích metod a legislativních překážek je její autentizační síla pouze průměrná.

3.1.16. Dynamika psaní a PIN

Popis metody: Během zadávání jména a hesla je sledována dynamika psaní daného uživatele, tím je tento jednoznačně identifikován.

Síla autentizace	Uživatelská přívětivost	TOC	Další aspekty
2,60	4,80	3,60	3,10

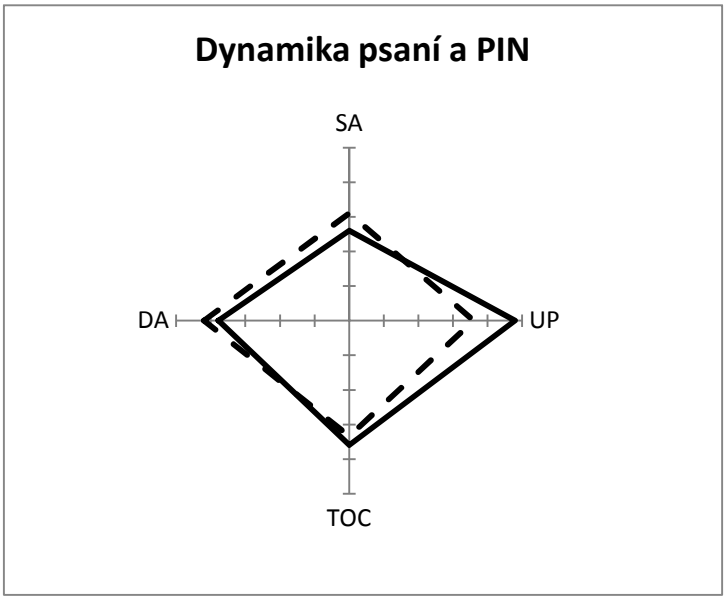
Tabulka 16: Vyhodnocení metody Dynamika psaní a PIN

Síla autentizace: Nižší úroveň zabezpečení způsobuje nedokonalost metod při rozpoznávání dynamiky ale i nedostatečná legislativní podpora.

Uživatelská přívětivost: Komfort, mobilita, jednoduchost použití jsou na velmi vysoké úrovni. Uživatel prakticky neví, že se autentizuje pomocí dynamiky psaní.

TOC: Průměrné náklady na provoz a implementaci.

Další aspekty: Požadavky na infrastrukturu jsou vyšší stejně tak i závislost na třetích stranách z důvodu použití sofistikovaných metod na identifikaci uživatele dle dynamiky psaní.



Obrázek 24: Vyhodnocení metody Dynamika psaní a PIN oproti průměrným výsledkům

Shrnutí: Metoda Dynamiky psaní přináší zajímavou možnost jak autentizovat uživatele bezpečnou cestou a zároveň nijak nenarušit uživatelskou přívětivost.

3.1.17. Vzájemné porovnání metod

Ze získaných hodnot lze vyčíst několik faktorů, které ovlivňují výsledné ohodnocení a vzájemné postavení autentizačních metod.

Jedním z opakujících se faktorů byla skutečnost, že metoda která nedisponuje příliš silnou úrovní zabezpečení vyniká v oblasti uživatelského komfortu (například autentizace jménem a heslem s použitím klasické i virtuální klávesnice).

Přesně opačný efekt, tedy vysokou bezpečnost a nízkou úroveň uživatelské přívětivosti lze pozorovat u novějších autentizační metod, používajících sofistikovanější způsoby autentizace (USB token s certifikátem, Čipová karta).

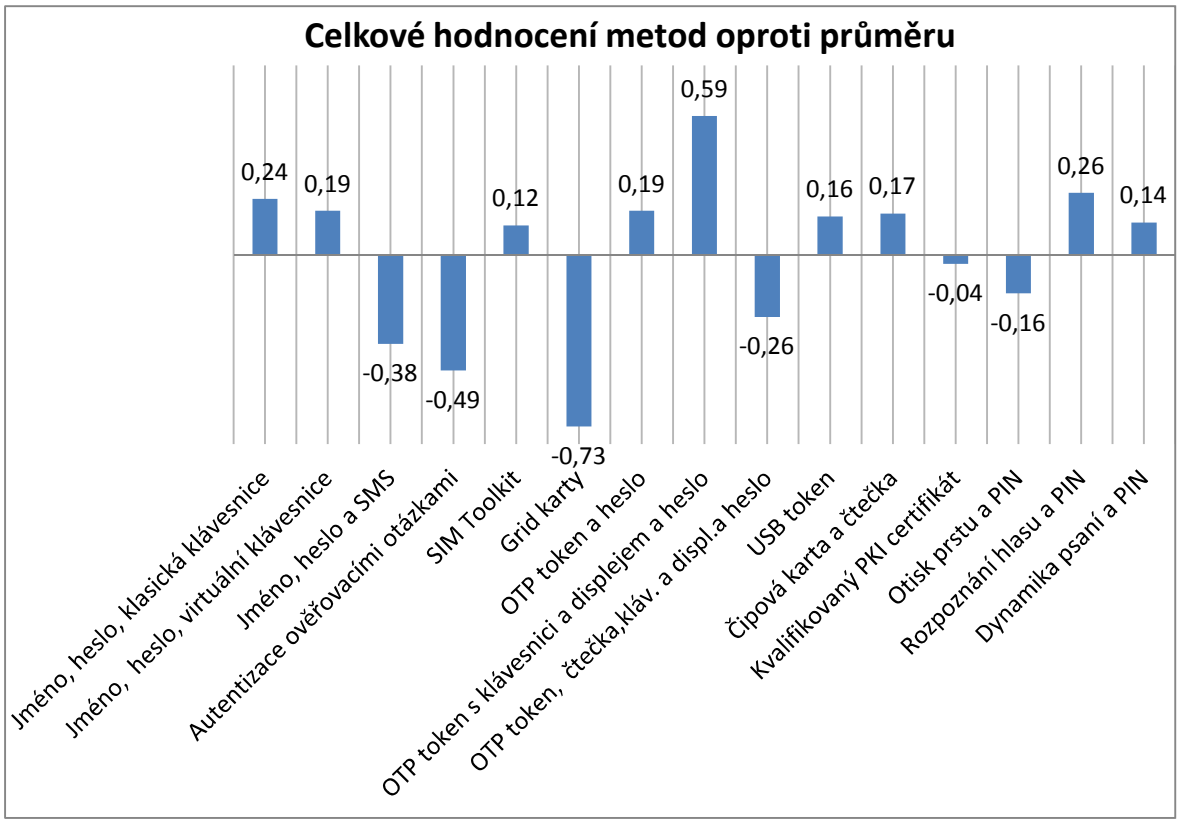
Pro moderní autentizační metody využívající biometrie je specifická silná závislost na třetích stranách, často doplněná o nízkou legislativní podporu a nedokonalost použitých metod a algoritmů.

Na grafu, který je zobrazen na obrázkuObrázek 25, jsou přehledně zobrazeny odchylky jednotlivých metod od průměrných hodnot získaných během analýzy.

Zajímavým poznatkem je, že se klasické autentizační metody (jméno a heslo) v celkovém hodnocení vyrovnají moderním metodám používajících biometrických prvků. To je způsobeno již zmíněným faktorem poměru dobré uživatelské přívětivosti a úrovně zabezpečení.

K nejbezpečnějším metodám patří použití jednorázových hesel a certifikátů, nesmí být ovšem doplněny o další nástroje, které ztěžují jejich použití a snižují mobilitu (čtečky).

Metoda Grid karet se stala nejhorší, zejména kvůli vysokým nákladům, nízké úrovni zabezpečení a v neposlední řadě netriviálností použití a s ní spojenou nekonformitou uživatele.



Obrázek 25: Celkové hodnocení metody oproti průměru

Výsledné hodnoty, z nichž vycházel předchozí text, naleznete v příloze Příloha C.

3.2. Návrh metody pro monitorování uživatelů

3.2.1. Úvod

Jak již bylo řečeno, metodám na bázi bezpečnostního monitoringu je přisuzována budoucnost zabezpečení přímého bankovnictví. Proto v této části své práce uvedu ukázkový příklad nasazení systému bezpečnostního monitoringu do reálného prostředí s dostupnými technologiemi.

Pro návrh metody pro monitorování uživatelů byl vybrán modelový příklad, ve kterém uživatel přistupuje k bankovním službám prostřednictvím internetového prohlížeče. Požadavky uživatele zpracovává aplikace internetového bankovnictví běžící na aplikačním serveru. Tyto požadavky jsou transformovány do podoby volání databázových procedur s příslušnými parametry nastavenými dle uživatelských požadavků.

Zjednodušené schéma modelového příkladu ukazuje obrázek Obrázek 26.

Obrázek 26: Zjednodušené schéma modelového příkladu

3.2.2. Popis architektury

Systém bezpečnostního monitoringu bývá nejčastěji postaven na analýze dat, která představují aktivitu uživatele v bankovním prostředí. Na takto získaná data jsou poté aplikována pravidla identifikující potenciálně nebezpečné události.

Protože aktivita uživatele způsobuje volání databázových procedur, představují tato volání s jejich parametry ideální vstupní data pro bezpečnostní monitoring.

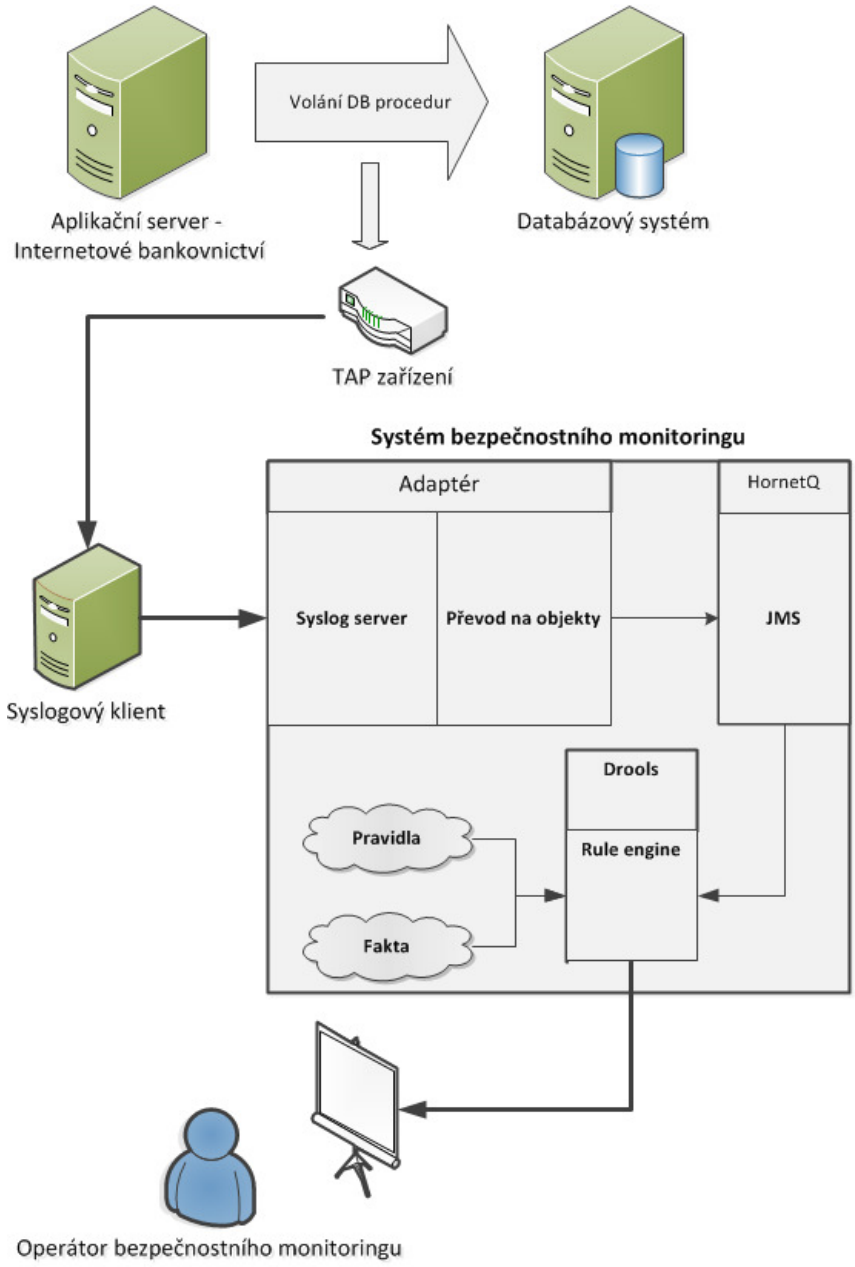
Pro zachycení databázových volání lze použít síťové *TAP* zařízení, které umožní přístup k síťovým datům procházejícím skrz něj. Data lze tedy duplikovat (zrcadlit) na jiné umístění, než bylo původně určené s minimálními výkonnostními vlivy.

Duplikovaná data je dále nutné nějakým způsobem přenést do systému bezpečnostního monitoringu. Pro svůj modelový příklad jsem vybral přenos pomocí technologie *Syslog*, avšak lze použít mnoho způsobů pro přenos informace vnitřní sítí.

Data z TAP zařízení tedy posílá syslogový klient na adaptér, který představuje syslogový server a je zodpovědný za převod syslogových zpráv na reálné objekty představující události volání databázových procedur. Další úkol adaptéru spočívá ve vkládání převedených a obohacených (časové údaje atd.) objektů do *JMS* (*Java message service*) fronty, která je součástí aplikačního serveru *JBoss*.

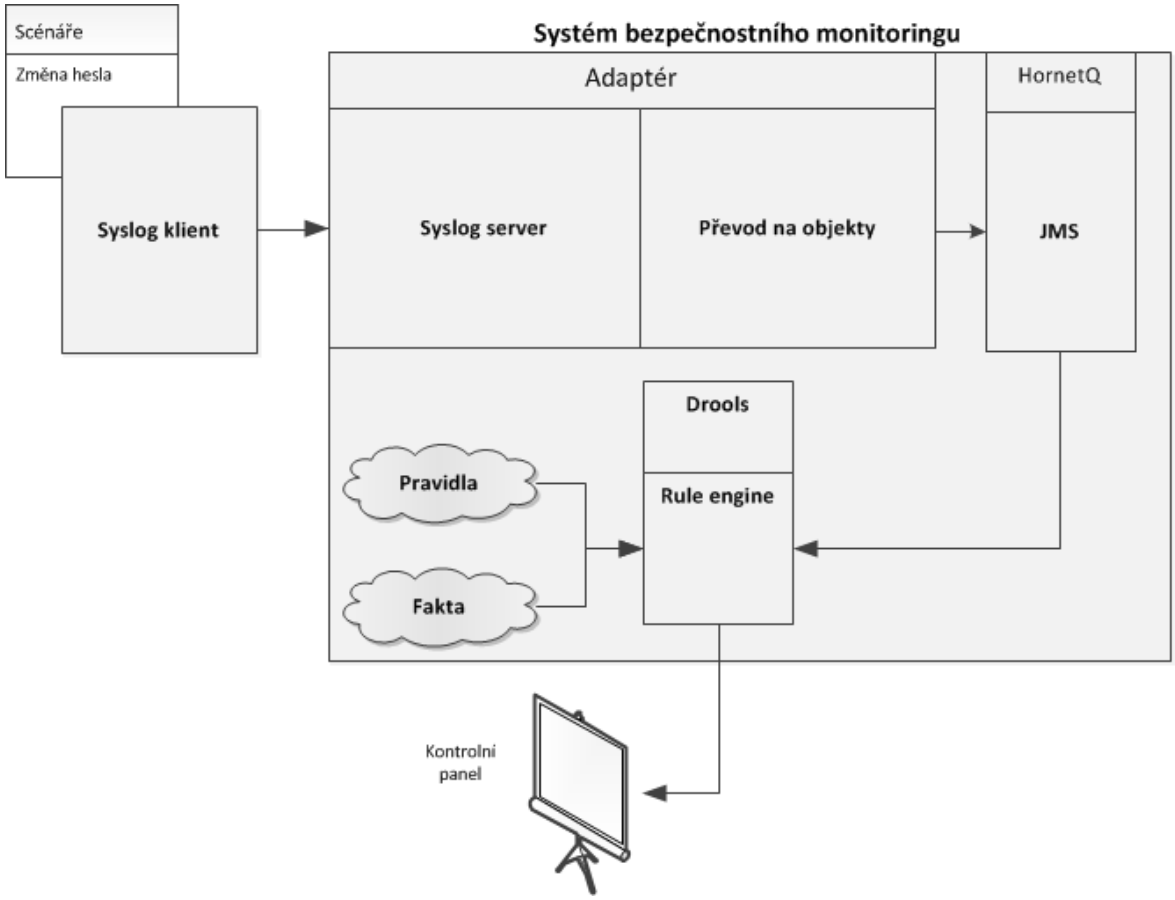
Zmíněná JMS fronta slouží jako vstup pro rozhodovací systém, v mém případě se jedná konkrétně o *JBoss Drools*, který obsahuje rozhodovací pravidla a poskytuje vstupní data pro kontrolní panel. Tento kontrolní panel představuje webové rozhraní pro operátory bezpečnostního monitoringu, které zobrazuje potenciálně nebezpečné události s jejich detaily a umožňuje operátorům reagovat na ně.

Schéma plnohodnotné architektury ukazuje obrázek Obrázek 27



Obrázek 27: Plnohodnotné schéma systému

Pro samotnou programátorskou realizaci jsem zvolil zjednodušené řešení (obrázekObrázek 28) výše zmíněné architektury a sice takové, které automaticky generuje vybrané databázové události (dle definovaných scénářů – viz dále), tedy syslogového klienta a dále se architektura podobá již zmíněné s tím rozdílem, že kontrolní panel, jež tvoří koncový bod systému, slouží pouze pro informativní účely a neposkytuje tak žádnou jinou funkcionalitu.



Obrázek 28: Realizace bezpečnostního monitoringu

Podrobnosti o jednotlivých částech systému budou uvedeny dále.

3.2.3. Použité technologie

V této sekci budou popsány technologie a systémy použité pro realizaci systému bezpečnostního monitoringu. Celá aplikace je napsána v jazyce Java a pro svůj běh vyžaduje JDK verze 1.6.

3.2.3.1. JBoss aplikační server

JBoss aplikační server poskytuje základní funkce programům v něm běžícím. Jedná se tedy o určitou abstraktní vrstvu jejímž účelem je umožnit jednoduší psaní aplikací.

V mém případě jsem JBoss využil pro jeho integraci JMS a s ní související technologií *HornetQ*, který představuje asynchronní systém pro posílání zpráv, tzv. *MOM* (*Message oriented middleware*) a poskytuje jednoduché rozhraní pro konfiguraci JMS front.

Způsob konfigurace HornetQ a JMS front naleznete na přiloženém DVD.

3.2.3.2. Syslog4j

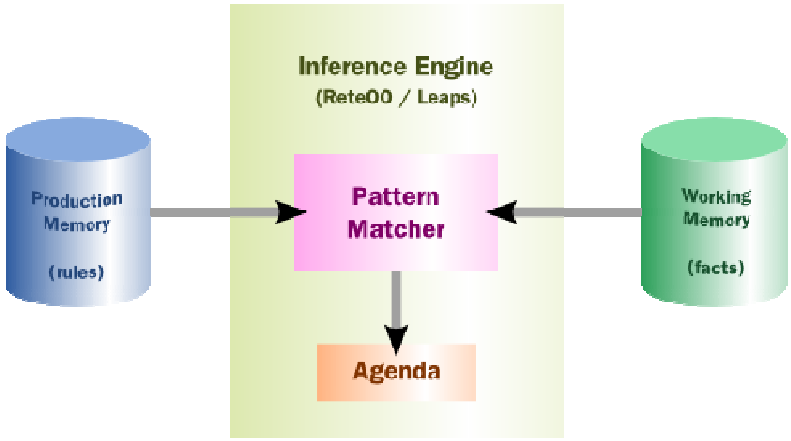
Syslog4j představuje kompletní klientskou i serverovou implementaci technologie syslog pro jazyk Java.

Syslog4j poskytuje jednoduché a snadno konfigurovatelné rozhraní pro zasílání zpráv mezi aplikacemi protokoly UDP a TCP.

3.2.3.3. JBoss Drools

JBoss Drools je platforma integrující business logiku, která představuje jednotnou platformu pro pravidla, workflow a zpracování událostí [DR].

Drools se skládají z několika funkčních modulů z nichž jsem pro svou práci vybral Drools Expert, který představuje systém založený na pravidlech, tzv. *Business rule engine*. Hlavním úkolem modulu Drools Expert je vyhodnocení a řízení pravidel.



Obrázek 29: Vysokoúrovňový pohled na rule engine [DR]

Produkční paměť, označovaná také jako báze znalostí, obsahuje pravidla se kterými systém pracuje. Pravidla jsou napsána formou speciálního jazyka, tzv. *DRL* (*Drools rule language*). Jak je vidět na obrázku Obrázek 30, pravidla vycházejí z jazyka Java.

```
rule "Uživatel je starší 18ti let"

when
     Osoba (věk >= 18)                          // podmínka
then
      System.out.println("Osoba je plnoletá");   // akce
end
```

Obrázek 30: Příklad jednoduchého pravidla

Pracovní paměť tvoří fakta. V Drools jsou takto označeny klasické Java objekty, neboli *POJO* (*Plain Old Java Object*). Tyto objekty je nutné nejprve deklarovat (obrázekObrázek 31) a až poté je můžeme použít při tvorbě pravidel.

```
declare Osoba
   věk : int
   jméno : String
   adresa : String
end
```

Obrázek 31: Deklarace jednoduchého faktu

Agendu tvoří tabulka již splněných (resp. aktivovaných) pravidel a umožňuje na ně provést reakci.

Popis celého systému Drools by byl příliš obsáhlý, stejně tak i princip a pravidla pro tvorbu pravidel, proto zde uvádím pouze základní informace. Ve své práci však používám základní, velice srozumitelné, prvky tohoto systému a k jejich pochopení stačí pouze prostudování dokumentovaného zdrojového kódu.

3.3. Struktura systému

Vytvořená aplikace simulující systém bezpečnostního monitoringu je rozdělena do tří samostatných modulů:

- **Client**
- **Adapter**
- **Common**
- **Rule engine**

Všechny moduly obsahují balíky, jejich společným prefixem je **cz.zcu.kiv.secmon**. Detailní informace o jednotlivých modulech a jejich struktuře budou uvedeny dále.

3.3.1. Client

Modul klient představuje abstrakci odchytávání volání databázových procedur a jejich posílání pomocí Syslogu.

Klient pouze generuje dle zadaných parametrů zprávy, které se svým obsahem podobají reálnému databázovému volání. Tyto zprávy, respektive jejich předlohy, jsou načítány z konfiguračního souboru a dle vstupních parametrů jsou vyplněny a odeslány (další podrobnosti viz kapitola o funkcionalitě systému).

Kořenovým balíkem je **client**, který je dále rozdělen:

- **jms** – také obsahuje jedinou třídu zajišťující připojení k JMS frontě a poskytuje metodu pro posílání zpráv do této fronty.
- **loader** – je složen z několika navzájem souvisejících tříd, jejichž hlavní funkčnost spočívá v načtení konfiguračních souborů. Tyto konfigurační soubory obsahují definice scénářů (více v kapitole 3.4). Umožňuje tak dle parametrů z příkazové řádky spouštět určité scénáře v definovaném pořadí, s daným počtem iterací a ve vícevláknovém režimu. K tomuto účelu je vytvořena hlavní třída, která se nazývá *SyslogLoaderMain*.
- **syslog** – obsahuje jedinou třídu představující syslogového klienta prostřednictvím technologie Syslog4j. Dále poskytuje metodu pro posílání syslogových zpráv.

3.3.2. Adaptér

Kořenovým balíkem celého Adaptéru je **adapter**. Tento je následně rozdělen dle funkcionality do několika dalších balíků:

- **server** – kromě implementace syslogového serveru obsahuje i třídu *SyslogJMSEventProcessor*, která slouží pro převod syslogových zpráv na objekty představující volání jednotlivých databázových procedur.
- **main –** obsahuje hlavní třídu pro spuštění Adaptéru.

Kromě nutných konfiguračních souborů (log4j, jms) je obsahem adresáři s konfigurací i složka *test*, v níž se nacházejí předlohy procedur, které slouží pro vygenerování událostí, jež zastupují skutečné volání databázových procedur.

3.3.3. Common

Modul Common (ve stejnojmenném balíku) obsahuje třídy definující jednotlivé objekty použité v systému bezpečnostního monitoringu. Modul je dále rozdělen:

- **eventmodel** dále se dělící na
  - **facts** – objektu představující fakta v systému rule engine
  - **messages** – objekty, které nahrazují volání databázových procedur a které slouží jako vstup pro rule engine
- **util** – pomocné třídy pro zpracování konfiguračních souborů

3.3.4. Rule engine

Webová aplikace obsahující jediný balík **rule.engine**, v němž jsou definovány celkem 3 třídy:

- *JMSConnector* - konektor pro načítání obsahu JMS fronty
- *Engine* – představuje samotný rule engine
- *ContextListener* – pro spuštění rule enginu na pozadí webové aplikace

Kromě nutných konfiguračních souborů (log4j,jms) obsahuje adresář s konfigurací i soubor *rules.drl* ve kterém jsou definována pravidla odpovídající scénářům.

Webová aplikace obsahuje pouze jediný JSP soubor – *index.jsp*, který představuje kontrolní panel (obrázek 32).

3.4. Funkcionalita systému

Jak již bylo řečeno v kapitole 3.2.2 tok dat ve zjednodušeném modelovém příkladu vypadá následovně:

1. Vygenerování syslogových zpráv (pomocí třídy *SyslogLoaderMain*) s definovanými parametry (počet iterací, výběr scénářů) a jejich odeslání syslogovým klientem.

2. Adaptér přijímá syslogová data, převede je na objekty, které nahrazují databázové procedury, a vloží je do JMS fronty.
3. Rule engine vybírá data z fronty a na jejich základě vyhodnocuje pravidla definovaná v externím souboru *rules.drl*.
4. Aktivovaná pravidla jsou zaznamenána a zobrazena v kontrolním panelu.

Ukázku kontrolního panelu zobrazuje obrázek Obrázek 32: Ukázka kontrolního panelu.

Security monitoring Control Panel

ID	Čas vytvoření	Severita	ID uživatele	Událost	IP adresa	Začátek incidentu	Konec incidentu
0	Mon May 07 10:45:39 CEST 2012	3	9il7gr5	Změna hesla uživatele na blacklistu	19216811	Mon May 07 10:45:39 CEST 2012	Mon May 07 10:45:39 CEST 2012
1	Mon May 07 10:46:08 CEST 2012	3	9il7gr5	Změna hesla uživatele na blacklistu	19216811	Mon May 07 10:45:39 CEST 2012	Mon May 07 10:45:39 CEST 2012
2	Mon May 07 10:48:12 CEST 2012	2	8mbq42	Autorizace transakce pomoci SMS	19216813	Mon May 07 10:48:12 CEST 2012	Mon May 07 10:48:12 CEST 2012
3	Mon May 07 10:48:12 CEST 2012	3	9il7gr5	Změna hesla uživatele na blacklistu	19216812	Mon May 07 10:48:12 CEST 2012	Mon May 07 10:48:12 CEST 2012
4	Mon May 07 10:48:28 CEST 2012	2	9il7gr5	Nastaveni SMS pro autentizaci	19216812	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
5	Mon May 07 10:48:28 CEST 2012	2	l20n7zs	Nastaveni SMS pro autorizaci	19216813	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
6	Mon May 07 10:48:28 CEST 2012	3	9il7gr5	Změna hesla uživatele na blacklistu	19216811	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
7	Mon May 07 10:48:28 CEST 2012	2	8mbq42	Autorizace transakce pomoci SMS	19216811	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
8	Mon May 07 10:48:28 CEST 2012	2	9il7gr5	Nastaveni SMS pro autentizaci	19216811	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
9	Mon May 07 10:48:28 CEST 2012	3	9il7gr5	Odblokování uživatelského hesla uživatele na blacklistu	19216811	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
10	Mon May 07 10:48:28 CEST 2012	2	l20n7zs	Nastaveni SMS pro autentizaci	19216811	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
11	Mon May 07 10:48:29 CEST 2012	2	l20n7zs	SMS verifikace při přihlášeni	19216811	Mon May 07 10:48:28 CEST 2012	Mon May 07 10:48:28 CEST 2012
12	Mon May 07 10:48:46 CEST 2012	2	l20n7zs	SMS verifikace při přihlášeni	19216812	Mon May 07 10:48:46 CEST 2012	Mon May 07 10:48:46 CEST 2012
13	Mon May 07 10:49:03 CEST 2012	2	9il7gr5	Nastaveni SMS pro autentizaci	19216811	Mon May 07 10:49:03 CEST 2012	Mon May 07 10:49:03 CEST 2012
14	Mon May 07 10:49:03 CEST 2012	2	l20n7zs	Autorizace transakce pomoci SMS	19216813	Mon May 07 10:49:03 CEST 2012	Mon May 07 10:49:03 CEST 2012
15	Mon May 07 10:49:11 CEST 2012	2	8mbq42	Autorizace transakce pomoci SMS	19216813	Mon May 07 10:49:11 CEST 2012	Mon May 07 10:49:11 CEST 2012
16	Mon May 07 10:49:11 CEST 2012	4	8mbq42	Transakce s částkou 50 000 Kč	19216813	Mon May 07 10:49:11 CEST 2012	Mon May 07 10:49:11 CEST 2012
17	Mon May 07 10:49:28 CEST 2012	4	8mbq42	Transakce s částkou 50 000 Kč	19216812	Mon May 07 10:49:28 CEST 2012	Mon May 07 10:49:28 CEST 2012
18	Mon May 07 10:49:28 CEST 2012	2	8mbq42	Autorizace transakce pomoci SMS	19216812	Mon May 07 10:49:28 CEST 2012	Mon May 07 10:49:28 CEST 2012
19	Mon May 07 10:49:44 CEST 2012	2	9il7gr5	Autorizace transakce pomoci SMS	19216812	Mon May 07 10:49:44 CEST 2012	Mon May 07 10:49:44 CEST 2012

Obrázek 32: Ukázka kontrolního panelu

Pro modelový příklad jsem nadefinoval 9 ukázkových scénářů, které (stejně jako struktura volaných procedur) vycházejí z reálného prostředí:

1. Změna hesla uživatele, který je na blacklistu
2. Odblokování hesla uživatele, který je na blacklistu
3. Nastavení SMS pro autentizaci
4. Nastavení SMS pro autorizaci
5. 5ti násobné úspěšné přihlášení uživatele během 3 minut
6. 5ti násobné neúspěšné přihlášení uživatele během 3 minut
7. Autentizace pomocí SMS

8. Autorizace transakce pomocí SMS
9. Vybraný uživatel poslal částku 50 000 Kč

Návod pro nastavení a spuštění aplikace bezpečnostního monitoringu naleznete na přiloženém DVD.

4. Závěr

V dnešním technologicky vyspělém světě je použití moderních bankovních kanálů již samozřejmostí. A právě s rostoucím počtem bankovních kanálů a jejich klientů stoupají i požadavky na zabezpečení. Proto vznikají nové autentizační metody, ale i jiné metody zajišťující uživatelskou bezpečnost při používání bankovních kanálů.

Během analýzy současných a moderních autentizačních metod jsem se setkal s opakujícím se jevem. Podstatou tohoto jevu byla skutečnost, že metoda, jejíž úroveň bezpečnosti byla nízká, poskytovala velmi vysoký uživatelský komfort. Jedná se o klasické autentizační metody, tedy například použití jména a jednoduchého hesla. Přesný opak poté nabízejí moderní bezpečnostní metody, které sice poskytují vysokou úroveň zabezpečení, ale z důvodu nutnosti použití dalších zařízení (například nejrůznějších čteček), nebo netriviálního autentizačního procesu (vložení USB tokenu, načtení certifikátu, zadání jména a hesla) je jejich uživatelský komfort značně snížen. V celkovém hodnocení se tedy rozdíly mezi klasickými a moderními metodami stírají.

Moderní autentizační metody ovšem nejsou jediným současným trendem v oblasti bezpečnosti bankovních kanálů. Stále větší pozornost je věnována systémům pro detekci anomálií, popř. systémům pro detekci chování uživatelů. Principem těchto systémů není zabránění neoprávněného přístupu k bankovním aplikacím, ale jeho odhalení. Na základě pozorování chování a prováděných akcí lze rozpoznat podezřelou událost, na kterou je poté upozorněn operátor bezpečnostního monitoringu, jež zareaguje podle stanovených scénářů a politik.

Právě systém pro monitorování uživatelů tvoří součást mé diplomové práce. Systém je založen na nástroji JBoss Drools, který poskytuje komplexní a bezplatnou platformu pro zpracování business logiky. Pravidla, na nichž je celý systém založen, zprostředkovávají vyhodnocení událostí vyvolaných uživatelem. Splněná pravidla lze poté dále využít pro adekvátní reakci ze strany operátorů. Realizovaný systém demonstruje možnosti použití systému pro monitorování uživatelů v reálném prostředí.

5. Přehled zkratek

3DES	„*Triple DES*“, bloková šifra založená na šifrování Data Encryption Standard (DES)
RC4	„*Rivest Cipher 4*", algoritmus používaný pro šifrovaný přenos
AES	„*Advanced Encryption Standard*”, symetrická bloková šifra nahrazující DES
IDEA	„*International Data Encryption Algorithm*”, symetrická bloková šifra
RSA	Algoritmus šifrování pomocí veřejného klíče
DSA	„*Digital Signature Algorithm*”, standard pro digitální podpisy
ECC	*Elliptic Curve Cryptography*, šifrování pomocí eliptických křivek
MD5	„*Message-Digest algorithm*“, algoritmus používající funkci hash
SHA-1	„*Secure Hash Algorithm*“, rozšířená hashovací funkce, která vytváří otisk pevné délky
SHA-2	Bezpečnější řešení SHA-1
X.509	Standard pro práci s certifikáty
DNS	„*Domain Name System*“, systém doménových jmen
MAC	„*Media Access Control*“, jedinečný identifikátor zařízení
ARP	„*Address Resolution Protocol*”, protokol pro získání MAC adresy
IP	„*InternetPprotokol*“, síťový komunikační protokol
SIM	„*Subscriber Identity Module*“, karta pro jednoznačnou identifikaci účastníka
SMS	„S*hort Mmessage Service*“, služba pro zasílání krátkých zpráv

PIN	„*Personal Identification Number*“, číslo jednoznačně identifikující osobu
TAN	„*Transaction Authentication Number*“, číslo pro autentizaci transakce
ECG	„*Electrocardiography*“, zachycení srdeční aktivity
EEG	„*Electroencephalography*“, zachycení mozkové aktivity
TCO	„*Total cost of ownership*“, celkové náklady na vlastnictví
JMS	„*Java messaging service“*, služba pro posílání zpráv mezi klienty
JDK	*„Java development kit“*, soubor nástrojů pro vývoj aplikací v jazyce Java
JSP	*„Java server pages“*, technologie pro vytváření dynamicky generovaných webových stránek
MOM	*„Message oriented middleware”*, softwarová architektura pro zasílání zpráv mezi systémy

6. Seznam použité literatury

[AP] APOSTOLOS ATH GKOUTZINIS: *Internet banking and the law in Europe: regulation, financial integration and electronic commerce*, Cambridge University Press, 2006, 354 s., ISBN: 0521860717

[MJC] MARY J. CRONIN: *Banking and Finance on the Internet*. Van Nostrand Reinhold, Indiana University, 1997, 334 s., ISBN 0471292192. Dostupné online na URL: < http://books.google.co.uk/books?id=l94FEs-lMu4C >

[STA] Statistická ročenka České republiky 2011. *Vybrané kapitoly prováděné jednotlivci na internetu,* kapitola 21-21 Dostupné online na URL: <http://www.czso.cz/csu/2011edicniplan.nsf/t/35001F0101/$File/000111 2121.xls>

[MŘ] MATYÁŠ VÁCLAV, ŘÍHA, ZDENĚK: *Autentizace a řízení přístupu – studijní materiá*l. Prezentace v IS MU, 2011, [27.2.2012], Dostupné online z URL:<http://is.muni.cz/el/1433/jaro2011/PV157/um/ PV157_2011_L1_Uvod_final.pdf?fakulta=1433;obdobi=5105;kod=PV157>

[LRG] Rick Lehtinen, Deborah Russell, G. T. Gangemi: *Computer security basics*.

O'Reilly Media, Inc., 2006, 296 s., ISBN 0596006691, 9780596006693.

Dostupné online na URL:< http://books.google.cz/books?id=fqCFfuAJ4uEC>

[ZA] Zákon ČNR č 277/2000 Sb. ze dne 29.6.2000 o elektronickém podpisu.

[FFIEC] FFIEC Federal Financial Institutions Examination Council, , *Frequently asked questions*, 2006. Dostupné online z URL: http://www.ffiec.gov/pdf/authen tication_faq.pdf

[BAR] J. BRAINARD, A.JUELS, R. L. RIVERST *FourthFactor Authentication: Somebody You Know*, 2006,. Dostupné online z URL: http://www.rsa.com/ rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf

[FFIEC1] FFIEC Federal Financial Institutions Examination Council, , *Supplement to Authentication in an Internet Banking Environment*, 2011. Dostupné online z URL: http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf

[DR] JBoss Drools, dostupné online http://www.jboss.org/drools

7. Přílohy

7.1. Příloha A – Tabulka kritérií

Metrika	Kritérium	Popis
Síla autentizace	Úroveň zabezpečení	Počet faktorů, kryptografická síla, minimalizace útoků
	Perspektiva metody	Bezpečnostní doporučení uznávanými orgány (EU, státní výbory)
Uživatelská přívětivost	Komfort uživatele	Intuitivnost metody, absence externích zařízení, snadná instalace
	Jednoduchost použití	Použitelnost pro všechny věkové skupiny
	Mobilita	Nezávislost na zařízení (uživatel může využít metodu na jiném systému)
	Finanční náročnost pro uživatele	Nutnost pořízení externích zařízení
	Sociální přijatelnost	Použití metod, postupů a zařízení, které jsou běžně používány
TOC	Cena implementace	Cena související s implementací metody
	Provozní cena	Cena za operace (sms, call centra), externí zařízení poskytované
Další aspekty	Závislost na třetích stranách	Závislost na mobilním operátorovi, CA
	Časová náročnost nasazení	Čas pro nastavení a nasazení metody
	Distribuce	Distribuce dat (přihlašovací jména, tokeny) k uživatelům
	Podpora	Obsluha klientských požadavků, zátěž call centra, obnova uživatelských dat
	Požadavky	Požadavky na hw. a sw. strukturu
	Životnost	Očekávaná životnost metody (tokenů, kryptografické síly)

7.2. Příloha B – Detailní popis stupnic jednotlivých kritérií

Metrika	Kritérium	Popis metody
Síla autentizace	Úroveň zabezpečení	Počet faktorů, kryptografická síla, minimalizace útoků
	Perspektiva metody	Bezpečnostní doporučení uznávanými orgány (EU, státní výbory)
Uživatelská přívětivost	Komfort uživatele	Intuitivnost metody, absence externích zařízení, snadná instalace
	Jednoduchost použití	Použitelnost pro všechny věkové skupiny
	Mobilita	Nezávislost na zařízení (uživatel může využít metodu na jiném systému)
	Sociální přijatelnost	Použití metod, postupů a zařízení, které jsou běžně používány
	Finanční náročnost pro uživatele	Nutnost pořízení externích zařízení
TOC	Cena implementace	Cena související s implementací metody
	Provozní cena	Cena za operace (sms, call centra), externí zařízení poskytované
Další aspekty	Závislost na třetích stranách	Závislost na mobilním operátorovi, CA
	Časová náročnost aktivace	Čas pro nastavení autentizační metody pro klienta
	Distribuce	Distribuce dat (přihlašovací jména, tokeny) k uživatelům
	Podpora	Obsluha klientských požadavků, zátěž call centra, obnova uživatelských dat
	Požadavky	Požadavky na hw. a sw. strukturu
	Životnost	Očekávaná životnost metody (tokenů, kryptografické síly)

1 (nejhorší)	2	3
Jednoduché heslo, údaje o uživateli	Vylepšené heslo	Dvoufaktorová autentizace a jednoduchý token
Jednoduché heslo, údaje o uživateli	Vylepšené heslo	Dvoufaktorová autentizace a jednoduchý token
Čtečky pro čipovou kartu, náhodně generovaná hesla	PKI autentizace	OTP generátory
Čtečky pro čipovou kartu připojené k systému	Připojené OTP tokeny	Nepřipojené tokeny s klávesnicí
Připojené čipové karty	Připojené OTP tokeny	Vylepšená hesla, nepřipojené tokeny
Čipové karty vyžadující čtečky	OTP Tokeny	SMS verifikace
Velmi drahá autentizační zařízení (čipová karta se čtecím zařízením)	Drahá zařízení (OTP tokeny)	Malá investice do autentizačních zařízení
Velmi vysoká investice do infrastruktury a zabezpečení (Biometrie)	Vysoká investice do infrastruktury, testování	Středně vysoká investice (OTP tokeny)
Velmi vysoké náklady (SMS)	Vysoká náklady (komplexní call centra)	Střední náklady (podpora call centra, připojené tokeny)
Třetí strana je odpovědná za online autentizaci	Třetí strana poskytuje pouze aktivační služby	Třetí strana poskytuje offline služby
Aktivace delší než 3 dny	Aktivace do 3 dnů	Aktivace následující pracovní den
Klient musí navštívit třetí stranu	Klient musí navštívit pobočku	Klient obdrží data poštovní službou
Velmi velká zátež call center během aktivace, nebo obnovy dat	Velká potřeba call centra a jeho velká vytíženost	Střední potřeba podpory call centra, případně jiné (online)
Velmi komplexní infrastruktury	Potřeba nové infrastruktury kvůli výkonovým a kapacitním nárokům	Střední vylepšení současné infrastruktury
2 roky	4 roky	6 let

4	5 (nejlepší)
Dvoufaktorová autentizace a komplexní token	Dvoufaktorová autentizace, jeden faktor biometrický
Dvoufaktorová autentizace a komplexní token	Dvoufaktorová autentizace, jeden faktor biometrický
Aplikace v mobilním telefonu	Jednoduchá hesla, biometrie
Nepřipojené tokeny bez klávesnice	Jednoduchá hesla, biometrie
Mobilní telefony	Jednoduchá hesla, biometrie
Autentizace pomocí mobilního telefonu	Jednoduché heslo
Minimální investice (mobilní aplikace)	Žádná investice
Malá investice (nepřipojené tokeny)	Velmi malá investice (jednoduché heslo)
Nízké náklady (podpora call centra, nepřipojené tokeny)	Velmi nízké náklady (jednoduché heslo)
Třetí strana poskytuje OTP tokeny, čipové karty	Žádná třetí strana
Aktivace v řádu hodin	Okamžitá aktivace
Klient obdrží data online cestou	Klient obdrží všechny data okamžitě na pobočce banky
Malé využití call centra, případně jiné podpory (online)	Minimální nutnost call centra,případně jiné podpory (online)
Malé vylepšení současné infrastruktury	Metoda nevyžaduje další vylepšení infrastruktury
8 let	10 let

7.3. Příloha C – Výsledné ohodnocení autentizačních metod

	Váhový koeficient	Jméno, heslo, klasická klávesnice	Jméno, heslo, virtuální klávesnice	Jméno, heslo a SMS	Autentizace ověřovacími otázkami	SIM Toolkit
Odchylka od průměru		**0,24**	**0,19**	**-0,38**	**-0,49**	**0,12**
Hodnocení		**3,63**	**3,58**	**3,01**	**2,90**	**3,51**
Síla autentizace		**1,00**	**1,30**	**3,60**	**1,00**	**3,00**
Úroveň zabezpečení	6	1,0	1,5	4,0	1,0	3,0
Perspektiva metody	4	1,0	1,0	3,0	1,0	3,0
Uživatelská přívětivost		**4,60**	**4,10**	**3,15**	**4,00**	**4,00**
Komfort uživatele	3	5,0	4,0	2,5	3,0	3,0
Jednoduchost použití	2	5,0	4,0	3,0	4,0	3,0
Mobilita	2	3,0	3,0	3,0	5,0	5,0
Sociální přijatelnost	1	5,0	5,0	4,0	3,0	5,0
Finanční náročnost pro uživatele	2	5,0	5,0	4,0	5,0	5,0
TOC		**5,00**	**5,00**	**1,80**	**3,40**	**3,60**
Cena implementace	4	5,0	5,0	3,0	4,0	3,0
Provozní cena	6	5,0	5,0	1,0	3,0	4,0
Další aspekty		**3,90**	**3,90**	**3,50**	**3,20**	**3,45**
Závislost na třetích stranách	2	5,0	5,0	1,0	5,0	2,0
Časová náročnost nasazení	1	5,0	5,0	5,0	5,0	3,0
Distribuce	1	5,0	5,0	5,0	5,0	1,5
Podpora	2	4,0	4,0	3,0	2,0	5,0
Požadavky	1	5,0	5,0	5,0	5,0	4,0
Životnost	3	2,0	2,0	4,0	1,0	4,0

Grid karty	OTP token a heslo	OTP token s klávesnici a displejem a heslo	OTP token, čtečka,kláv. a displ.a heslo	USB token	Čipová karta a čtečka	Kvalifikovaný PKI certifikát	Otisk prstu a PIN	Rozpoznání hlasu a PIN	Dynamika psaní a PIN	Průměr
-0,73	**0,19**	**0,59**	**-0,26**	**0,16**	**0,17**	**-0,04**	**-0,16**	**0,26**	**0,14**	**3,39**
2,66	**3,58**	**3,98**	**3,13**	**3,55**	**3,56**	**3,35**	**3,23**	**3,65**	**3,53**	
2,20	**3,40**	**5,00**	**4,30**	**4,60**	**4,60**	**3,00**	**5,00**	**3,00**	**2,60**	
3,0	3,0	5,0	4,5	5,0	5,0	3,0	5,0	3,0	3,0	
1,0	4,0	5,0	4,0	4,0	4,0	3,0	5,0	3,0	2,0	
2,45	**3,80**	**3,90**	**2,00**	**2,90**	**3,10**	**3,50**	**2,80**	**5,00**	**4,80**	
1,5	4,0	3,0	2,0	3,0	3,0	4,0	3,0	5,0	5,0	
2,0	4,0	3,0	2,0	3,0	2,5	3,0	5,0	5,0	4,0	
3,0	5,0	5,0	2,0	4,0	2,5	2,0	1,0	5,0	5,0	
2,0	4,0	4,0	2,0	2,0	4,0	3,0	3,0	5,0	5,0	
4,0	2,0	5,0	2,0	2,0	4,0	5,0	2,0	5,0	5,0	
3,00	**3,60**	**3,60**	**3,00**	**3,00**	**3,00**	**2,80**	**2,00**	**3,60**	**3,60**	
3,0	3,0	3,0	3,0	3,0	3,0	4,0	2,0	3,0	3,0	
3,0	4,0	4,0	3,0	3,0	3,0	2,0	2,0	4,0	4,0	
3,00	**3,50**	**3,40**	**3,20**	**3,70**	**3,55**	**4,10**	**3,10**	**3,00**	**3,10**	
3,0	3,0	3,0	3,0	4,0	2,0	4,5	1,0	1,0	1,0	
5,0	5,0	5,0	5,0	4,0	5,0	5,0	4,0	5,0	5,0	
1,0	2,0	2,0	2,0	4,0	4,0	4,0	3,0	5,0	5,0	
2,0	3,0	3,0	2,0	3,0	3,0	3,0	3,0	3,0	4,0	
5,0	4,0	3,0	3,0	3,0	3,0	2,0	4,0	3,0	2,0	
3,0	4,0	4,0	4,0	4,0	4,5	5,0	4,0	3,0	3,0	