ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní

BAKALÁŘSKÁ PRÁCE

Prescreening
se vstupem z moderních technologií

Matouš Staněk

2014

Prohlášení

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

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

V Praze, dne 28. listopadu 2014

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
d ě k a n
Konviktská 20, 110 00 Praha 1

K621..... **Ústav letecké dopravy**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Matouš Staněk

Kód studijního programu a studijní obor studenta:

B 3710 – LED – Letecká doprava

Název tématu (česky): **Prescreening se vstupem z moderních technologií**

Název tématu (anglicky): Prescreening with Inputs from Modern Technologies

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte osnovou uvedenou v následujících bodech:

- Úvod
- Prescreening
- Technologie pro získávání informací
- Model
- Vyhodnocení navrženého modelu
- Závěr

Rozsah grafických prací: dle pokynů vedoucího bakalářske práce

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: J. Price, J. Forrest: Practical Aviation Security: Predicting and Preventing Future Threats

Předpis L17

Elias, B.: Airport and Aviation Security

Vedoucí bakalářské práce: **Ing. Jakub Kraus**

Ing. Peter Vittek

Datum zadání bakalářské práce: **23. října 2013**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **30. listopadu 2014**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Daniel Hanus, CSc.
vedoucí
Ústavu letecké dopravy

prof. Dr. Ing. Miroslav Svítek
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Matouš Staněk
jméno a podpis studenta

V Praze dne ..... 25. září 2014

Poděkování

Děkuji vedoucímu této bakalářské práce panu Ing. Jakubu Krausovi za pomoc, ochotu a vstřícnost a své rodině.

Bibliografická identifikace

Jméno a příjmení autora: Matouš Staněk

Název bakalářské práce: Prescreening se vstupem z moderních technologií

Škola: České vysoké učení technické v Praze, Fakulta dopravní

Vedoucí bakalářské práce: Ing. Jakub Kraus

Rok obhajoby bakalářské práce: 2015

Abstrakt:

Práce se snaží přispět ke zvýšení efektivity zajištění bezpečnosti letecké dopravy. Popisuje současné přístupy k prescreeningu, zkoumá možnosti jejich obohacení některými technologiemi vyvíjenými v rámci projektu INDECT a navrhuje model fungování takto vzniklého systému. Bylo zjištěno, že využití dvou ze čtyř zkoumaných technologií v prescreeningu je docela možné v jejich současné podobě, vyžaduje si však spolupráci se zpravodajskými službami. Využití ostatních dvou technologií je podmíněno jejich zdokonalením a přizpůsobením.

Klíčová slova:

zabezpečení civilního letectví, prescreening, INDECT

Bibliographic identification

Name and Surname of author: Matouš Staněk

Title of Bachelor work: Prescreening with inputs from modern technologies

University: Czech Technical University in Prague, Faculty of Transportation Sciences

Head of Bachelor work: Ing. Jakub Kraus

Year of habilitation: 2015

Abstract:

This thesis aims to contribute to increasing of efficiency in providing aviation security. It describes current approaches to prescreening, explores the possibilities of their enrichment by some technologies developed under INDECT project and proposes a model of such system. It was found that the use of two of the four examined technologies in prescreening is quite possible in their current form, but requires cooperation with intelligence services. The use of the other two technologies is conditioned by their improvement and adaptation.

Keywords:

aviation security, prescreening, INDECT

OBSAH

Seznam použitých zkratek

Zkratka	Anglický význam	Český význam
ACE	Automatic Content Extraction	Automatická extrakce obsahu
ALARP	As Low As Reasonably Practicable	Tak nízké, jak je to rozumně proveditelné
API	Advanced Passenger Information	Rozšířené informace o cestujících
APIS	Advanced Passenger Information System	Systém rozšířených informací o cestujících
APU	Auxiliary Power Unit	Pomocná energetická jednotka
CAPS	Computer-Assisted Aviation Prescreening System	Počítačový letecký prescreeningový systém
CAPPS	Computer-Assisted Passenger Presceening System	Počítačový systém prescreeningu cestujících
CBP	Customs and Border Protection	Úřad pro cla a ochranu hranic USA
CCTV	Closed Circuit Television	Uzavřený televizní okruh
DHS	Department of Homelad Security	Ministerstvo pro vnitrní bezpecnost
EDC	Entity Detection & Characterization	Detekce a charakterizace entit
FAA	Federal Aviation Administration	Federální letecká správa
FBI	Federal Bureau of Investigation	Federální úřad pro vyšetřování
GAO	Government Accountability Office	(nepřekládá se)
IATA	International Air Transport Association	Mezinárodní asociace leteckých dopravců
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
ICCAIA	International Coordinating Council of Aerospace Industries Associations	Mezinárodní koordinační rada asociací leteckého průmyslu
KBP	Knowledge Based Population	(nepřekládá se)
KTN	Known Traveler Number	Číslo důvěryhodného cestujícího
LNK	Entity Linking Tracking	Sledování propojení entit
NGen	Next Generation screening	Screening další generace
Pan Am	Pan American World Airways	(nepřekládá se)
PFLP	Popular Front for the Liberation of Palestine	Lidová fronta pro osvobození Palestiny
PNR	Passenger Name Record	Záznam o jméně cestujícího
RDC	Relation Detection & Characterization	Detekce a charakterizace vztahů
RE	Relation Extraction	Extrakce vztahů
SFPD	Secure Flight Passenger Data	Data o pasažérech v systému Secure Fl.

TSA	Transportation Security Administration	Úřad pro bezpečnost v dopravě
TSDB	Terrorist Screening Database	Databáze teroristů
UK	United Kingdom of Great Britain and Northern Ireland	Spojené království Velké Británie a Severního Irska
USA	United States of America	Spojené státy americké
WTC	World Trade Center	Světové obchodní centrum

Úvod

Po notoricky známých teroristických útocích na New York a Washington 11. září 2001, pro něž byla zneužita civilní letadla, došlo k významnému zpřísnění bezpečnostních kontrol cestujících v letecké dopravě. Toto zpřísnění však pro cestující znamená nejen snížení pohodlí, ale také nezanedbatelné zdržení. Hlavní výhoda letecké dopravy, její rychlost, tak do určité míry bere za své.

Některé odhady hovoří o zdvojnásobení současného počtu letecky přepravených cestujících do roku 2030. Ať už si o realističnosti těchto odhadů myslíme cokoliv, v případě, že by se naplnily, současný přístup k bezpečnostním kontrolám by se stal pravděpodobně neúnosným a paralyzujícím. Jsou proto vyvíjeny snahy, jak jej zefektivnit.

Jedním z výsledků těchto snah je koncept prescreeningu, jehož cílem je zjistit o pasažérovi co nejvíce z hlediska bezpečnosti relevantních informací ještě před provedením screeningu (detekční kontroly) na letišti.

Prescreening je v současnosti využíván pouze v USA a Izraeli. Cílem této bakalářské práce je zmapovat vývoj a stav prescreeningu v těchto státech a státech Evropské unie, kde je jeho zavedení plánováno, a navrhnout univerzální model, v němž by byly presceeningu nápomocny moderní bezpečnostní technologie.

Považuji za vhodné a ekonomicky optimální za tímto účelem prozkoumat možnosti použití některých součástí systému INDECT, který je dotován Evropskou unií částkou bezmála 15 milionů Eur.

Vzhledem k tomu, že v dané věci jde o poměrně zásadní zásahy do soukromí osob, rád bych se také stručně dotkl otázky ochrany lidských práv.

1 Zajištění bezpečnosti letecké dopravy

Tvrzení, že bezpečnost má nejvyšší prioritu, se může v prostředí všudypřítomné ekonomické soutěže, kde rozhoduje zisk, jevit jen jako reklamní slogan. Letectví je však jednou z oblastí, kde uvedené tvrzení snad stále ještě platí. Kromě upřímné snahy pracovníků v leteckém provozu je to dáno i tím, že selhání v zajištění bezpečnosti má ve svém důsledku i závažné ekonomické dopady (které mohou vyústit i v krach letecké společnosti), ale také poměrně značnou regulací a dohledem ze strany úřadů.

Na druhou stranu přílišná regulace a předpisová přísnost rovněž může vést k ekonomické devastaci leteckého průmyslu. Je tudíž třeba najít správnou míru minimalizace rizik, pročež byl zaveden přístup As Low As Reasonably Possible/Practicable (ALARP). Znamená to, že rizika mají být minimalizována do té míry, do jaké je to rozumně možné a proveditelné.

Při pojednání o bezpečnosti je třeba hned od počátku rozlišit dva pojmy užívané v letecké literatuře, *safety* a *security*. Třebaže čeština oba překládá jako *bezpečnost*, jejich význam je poněkud odlišný.

Safety znamená provozní bezpečnost ve smyslu absence leteckých nehod a incidentů vzniklých selháním techniky či lidského činitele.

Security znamená bezpečnost ve smyslu ochrany před protiprávními činy, jimiž se rozumí úmyslné poškození techniky, zranění, zabití či narušení plynulosti provozu.

Tato práce se zabývá bezpečností letecké dopravy v oblasti security. Nebude-li uvedeno jinak, bude v ní nadále pojem bezpečnost užíván vždy v tomto užším smyslu.

1.1 Právní zakotvení

V důsledku letecké kriminality a za účelem jejího potlačení byla v uplynulých desetiletých přijata celá řada opatření. Sluší alespoň velmi stručně předestřít, jak je pojednávané téma legislativně uchopeno.

Chicagská úmluva a předpisy řady L

V mezinárodní rovině je základní právní úpravou letecké bezpečnosti (security) ICAO Annex 17 – Ochrana mezinárodního civilního letectví před protiprávními činy, který je podobně jako ostatní přílohy k Chicagské úmluvě jakýmsi vzorem pro legislativy členských států ICAO, přičemž se doporučuje, aby letecké předpisy jednotlivých států byly přísnější než tyto minimální požadavky. V České republice odpovídá Annexu 17 předpis L17.

Z hlediska našeho tématu stojí za pozornost, že v tomto předpisu je definován pojem screening (detekční kontrola) jako „Aplikace technických nebo jiných prostředků, které mají za úkol odhalit zbraně, výbušniny a jiná nebezpečná zařízení nebo látky, kterých je možno použít pro spáchání protiprávního činu." (L17, Hlava 1)

Pojem **prescreening** v předpisu definován není, ale je nabíledni, že je to činnost, která screeningu předchází a s ním souvisí.

Našeho tématu se dotýká rovněž Annex 9 – Zjednodušení formalit (resp. předpis L9), jenž ukládá povinnost nemařit základní přednost letecké dopravy – její rychlost – při postupech prováděných při bezpečnostních kontrolách. Tím nepřímo vybízí k nalezení, rozvinutí a využití prostředků jako je prescreening.

1.2 Stručný přehled a historie protiprávních činů v letectví

Latinské přísloví praví: *Historia magistra vitæ*; a skutečně, má-li být zajištěna bezpečnost letectví v přítomnosti a budoucnosti, je i pro účely této práce užitečné podívat se, jak byla ohrožována v minulosti, jaké byly motivy osob, které protiprávní činnost provádí a jaké byly jejich metody.

Z hlediska kriminálních činů se někdy letecká historie rozděluje do tří fází:

- úniky před pronásledováním (1948-1968),
- politicky motivované činy (1968-1994),
- použití letadla jako zbraně (od r. 1994).

1.2.1 Úniky před pronásledováním (1948-1968)

V první fázi byla nejčastějším motivem únosů letadel snaha osob o únik před pronásledováním ze strany politického režimu. Jednalo se především o únosy z komunistických států, nejčastěji ze zemí Sovětského svazu a jejich satelitů do západní Evropy a z Kuby do USA. První takový únos provedli 6. dubna 1948 tři členové posádky a 21 z 26 pasažérů letu Československých aerolinií z Prahy, který místo v Bratislavě přistál v Mnichově.

Tyto únosy zpravidla nebyly provázeny závažnými škodami na lidských životech či technice. Na unesená letadla zde jejich únosci nahlíželi především jako na dopravní prostředek k úniku, jímž řešili svou osobní potřebu uniknout z totalitního režimu, nejednalo se tedy primárně o snahu vzbudit pozornost například k nějakému politickému poselství. Přesto však tyto únosy měly z hlediska politického jistý význam, neboť státy, z nichž se prchalo, neměly zájem na tom, aby o nich bylo známo, že pronásledují své občany. Přijímaly proto přísná bezpečnostní opatření. Nejenže se zpřísnily kontroly na letištích, které střežily ozbrojené složky, ale výkonní letci (kteří nezřídka byli sami únosci či jejich spolupracovníky) byli sledováni tajnou policií a mnozí z nich pracovali jako její agenti či důvěrníci podávající informace o svých kolezích.

Mezi Kubou a USA byla po sérii únosů v 60. letech 20. století uzavřena bilaterální smlouva o vydávání únosců. Postupně byly na letištích zaváděny detektory kovů. Z hlediska (pre)screeningu cestujících zvláště stojí za pozornost, že bezpečnostní složky USA v této době pracovaly na vytvoření profilu typického únosce ve snaze vytipovat podezřelé cestující na základě jejich chování před nástupem do letadla. Je to počátek behaviorální analýzy, která je od 70. let 20. století využívána při bezpečnostních kontrolách zvláště v Izraeli. Dá se předpokládat, že tato metoda se bude dále rozvíjet i v budoucnu.

1.2.2 Politicky motivované činy (1968-1994)

Za počátek druhé fáze leteckého zločinu se považuje únos letu 426 izraelských státních aerolinií El Al z Říma do Tel Avivu 26. července 1968. Tři únosci z Lidové fronty pro osvobození Palestiny (Popular Front for the Liberation of Palestine, zkráceně PFLP) za pomoci pistolí a ručních granátů přinutili posádku Boeingu 707 k diverzi do Alžírska, kde byli někteří cestující a členové posádky drženi jako rukojmí. Únosci je po pěti týdnech propustili výměnou za propuštění 16 odsouzených teroristů.

V září 1970 následovala série únosů, kdy PFLP unesla 4 letadla (celkem 577 cestujících a 39 členů posádky). Požadovala po vládách Švýcarska, Německa, Velké Británie a Izraele propuštění arabských zajatců. V dalších letech si tuto taktiku osvojily další teroristické skupiny na celém světě, takže v letech 1967 až 1996 z 1033 incidentům proti leteckých společnostem bylo 917 únosů, což je 88 %. [16]

Na rozdíl od předchozí fáze lze v této etapě už hovořit o terorismu v pravém smyslu slova (terreo – lat. děsit). Letadla zde už nejsou využívána jako prostředek dopravní, ale jako prostředek politického nátlaku. Cíle těchto kriminálních činů lze rozdělit následovně:

- ponížení nepřítele (jiných teroristických organizací nebo vlád států),
- způsobení ekonomické újmy nepřátelskému státu,
- použití jako nástroje vydírání za účelem propuštění spřízněných osob a/nebo finančního zisku.

Z hlediska následně přijatých bezpečnostních opatření (o nichž bude pojednáno v následující kapitole) je významný útok na letoun společnosti Pan Am, jehož trosky dopadly do oblasti Lockerbie ve Skotsku. Atentát byl proveden v roce 1988 pomocí plastické trhaviny československého původu Semtex, vložené do radiopřijímače umístěného do kufru v zavazadlovém prostoru, který nepatřil nikomu z cestujících na palubě.

1.2.3 Použití letadla jako ničícího nástroje (od r. 1994)

Za počátek třetí fáze je považován únos letu Air France 8969 Alžír – Paříž. Čtyři ozbrojení muži oblečení do uniforem alžírské policie nastoupili na alžírském letišti do letadla a jali se kontrolovat pasy cestujících. Palubní průvodčí odhalila, že jde o teroristy, leč ti si po 39 hodinách od zahájení únosu pod pohrůžkou zavraždění jednoho cestujícího každých 30 minut vynutili odlet. Kvůli nepřetržitě běžícímu APU (Auxiliary Power Unit) však neměli dostatek paliva pro let do Paříže, což si vyžádalo mezipřistání v Marseille, kde byli přeživší cestující a členové posádky vysvobozeni a teroristé zabiti.

Tento teroristický čin je převratný v tom, že, jak se zjistilo, únosci měli v plánu nechat letadlo vybuchnout nad Paříží (snad nad Eiffelovou věží či Elysejským palácem). Letadlo už nebylo hlavním cílem útoku, ale nástrojem k útoku na nejvýznamnější budovy v zemi.

Stejného charakteru byl i známý teroristický útok 11. září 2001, kdy byly v USA uneseny čtyři letouny a byly použity jako řízené střely, které zasáhly výškové budovy WTC v New Yorku a sídlo Ministerstva obrany, tzv. Pentagon, ve Washingtonu D. C.

Mezinárodní i státní instituce na tyto útoky relativně rychle reagovaly výrazným zpřísněním opatření v oblasti letecké bezpečnosti.

1.3 Obrana před protiprávními činy

Obrana před kriminálními činy vůči civilnímu letectví spočívá především v nevpuštění zločince na palubu letounu. Hlavním prostředkem k rozpoznání takového člověka mezi cestujícími je bezpečnostní kontrola provedená před nástupem cestujícího do letadla. Empiricky je zjištěno, že útoky na leteckou dopravu jsou nejčastěji prováděny s pomocí předmětů, které si útočníci přinesou na palubu. Bezpečnostní kontrola tedy spočívá převážně v detekci prostředků, kterými by mohl být protiprávní čin na palubě letadla spáchán.

Tento způsob zajištění bezpečnosti s sebou nese i některá úskalí, z nichž asi nejvýznamnější jsou tato:

1. protiprávní čin může být spáchán i s využitím předmětů, které buď nejsou vůbec detekovány, nebo projdou kontrolou nejsouce shledány jako nebezpečné, třebaže patřičně cvičené osoby by byly schopny je jako nebezpečné zbraně použít (keramický nůž, rybářský vlasec, těžký stativ fotoaparátu apod.)
2. podrobná a dlouhotrvající detekční kontrola zatěžuje systém snížením jeho efektivity a také může způsobovat únavu zaměstnanců kontrolu provádějících, kteří jsou tak více náchylní k chybám

První zmíněný problém je v současnosti řešen namátkovými osobními kontrolami cestujících, ovšem je to řešení pouze částečné. Třebaže může možnost namátkové kontroly část útočníků odradit (otázkou zůstává, jak velká ona část je), nezaručí jistotě se blížící pravděpodobnost odhalení nebezpečí. Navíc zhoršuje druhý zmíněný problém.

Řešením zvyšujícím efektivitu zajištění bezpečnosti je například prescreening, tedy prověření cestujících ještě před podstoupením běžného screeningu (detekční kontroly). Bude o něm pojednáno v následujících kapitolách.

2 Prescreening

Jak už bylo výše jinými slovy naznačeno, prescreening v letecké bezpečnosti se dá definovat jako proces pro zjišťování a ohodnocení (odhad) bezpečnostního rizika cestujícího před příchodem na bezpečnostní prohlídku na letišti. Zjednodušeně se tedy dá konstatovat, že proces prescreeningu rozdělí cestující do skupin dle míry rizika, které představují.

Pasažéři ohodnoceni jako nízkorizikoví mohou procházet jen elementární bezpečnostní prohlídkou (což snižuje časové nároky a náklady na zajištění bezpečnosti), naproti tomu u cestujících s vyšší hodnotou rizika personál letiště provede důkladnější bezpečnostní prohlídku, případně jsou zcela vyloučeni z přepravy. Tím má prescreening zvýšit pravděpodobnost odhalení hrozby a současně zefektivnit proces zajištění bezpečnosti.

2.1 Vývoj a současná podoba prescreeningu v USA

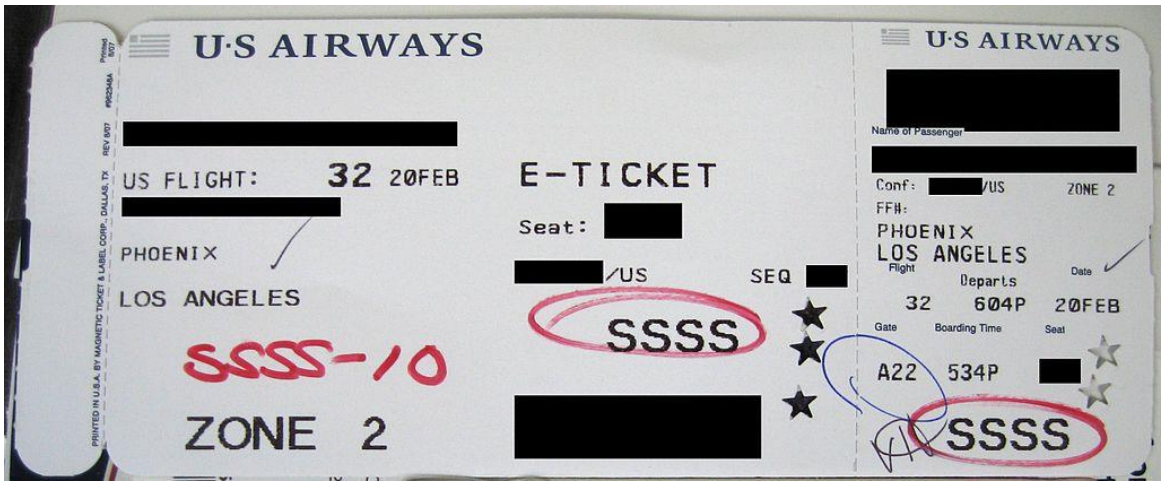
2.1.1 No Fly list

Útok na let 103 společnosti Pan Am nad Lockerbie v roce 1988 přiměl FAA k hledání nových možností zvýšení letecké bezpečnosti. Roku 1990 vláda Spojených států amerických podnítila vznik „No Fly list", tedy seznamu osob považovaných za bezpečnostní hrozbu pro civilní letectví, kterým nemá být umožněno dostat se na palubu letadla letícího do USA, z USA nebo v rámci USA. Do listopadu 2001 byl spravován FBI, poté jeho správu převzala Federal Aviation Administration (FAA).

Později byla administrací seznamu pověřena Transportation Security Administration (TSA), která umisťuje osoby do seznamů („No Fly" a „Automatic Selectee") na základě podnětů od zpravodajských služeb a seznamy předává leteckým dopravcům, jejichž úlohou je porovnat údaje pasažérů s těmito seznamy před jejich nástupem do letadla.

Jak plyne z informacích zmíněných v předcházejícím odstavci, původní No Fly byl rozdělen na seznamy „No Fly" a „Automatic Selectee". Osobám vyskytujícím se na

druhém jmenovaném seznamu je nástup na palubu umožněn po uspokojivém absolvování „sekundární bezpečnostní prohlídky“ (Secondary Security Screening), která je intenzivnější než primární kontrola. [7]



Obr. 1 – Palubní vstupenka cestujícího vybraného pro sekundární bezpečností prohlídku (Secondary Security Screening Selectee); Zdroj: [26]

2.1.2 Terrorist Screening Database (TSDB)

Vyšetřovací komise teroristických útoků z 11. září 2001 doporučila, aby pro prescreening pasažérů v letecké dopravě byl využíván i další seznam, Terrorist Screening Database, který obsahuje přes 1 000 000 záznamů a je spravován Terrorist Screening Center spadajícím pod FBI.

2.1.3 Computer-Assisted Aviation Prescreening System (CAPS)

CAPS je zkratkou slov Computer-Assisted Aviation Prescreening System. Jde o protiteroristický systém vyvíjený v USA, jenž využíval PNR (Passanger Name Record), což je záznam v databázi obsahující jméno a adresu cestujícího a informace o jeho objednaných letenkách. Tyto údaje byly porovnány s databázemi nebezpečných a hledaných osob (No-Fly list, TSDB apod.). Cestujícím bylo na tomto základě přiřazováno hodnocení dle rizika, které představují, a vysoce rizikoví cestující jsou podrobeni důkladnější bezpečnostní kontrole.

Systém byl vyvíjen od roku 1996 a byl v USA nasazen od dubna 1999. Později byl přejmenován na **CAPPS** (Computer-Assisted Passenger Presceening System). Systém CAPPS spolupracoval přímo s rezervačními systémy aerolinií (Amadeus apod.), konkrétní data tedy nepodléhala ani vládní, ani veřejné kontrole.

Během teroristických útoků unesenými letadly na New York a Washington D. C. v roce 2001 CAPPS zařadil 9 z 19 únosců mezi vysoce rizikové a byla u nich provedena důkladnější kontrola zavazadel, ovšem důkladnější osobní prohlídka nebyla provedena, což bylo v té době standardní, a únosci se tak dostali na paluby. Na základě této zkušenosti byl CAPPS změněn tak, že na základě určitých charakteristik získaných z PNR identifikuje i pasažéry pro intenzivnější osobní prohlídku.

2.1.4 CAPPS II

Roku 2003 předložila TSA návrh rozšíření systému CAPPS pod označením CAPPS II. Systém se opíral o PNR rozšířený o některá další data (datum narození, telefonní číslo…) a porovnával jej s vládními i nevládními databázemi za účelem spolehlivé identifikace osoby. Poté cestujícímu přiřadil jedno ze tří barevných označení dle stupně rizika, které by bylo vytištěno na palubní vstupence. Kritéria a metodika výpočtu rizika podléhají utajení a nikdy nebyly veřejně publikovány mimo TSA. Vešlo však v obecnou známost, že ke skupině pro dodatečnou kontrolu byli zařazováni cestující, kteří si koupili pouze jednosměrnou letenku, platili za ni v hotovosti nebo si ji kupovali na poslední chvíli.

Na CAPPS II se poměrně záhy snesla kritika ze strany lidskoprávních organizací a v roce 2004 Kongres USA rozhodl o zastavení jakéhokoliv financování systému, dokud nebude přezkoumán vládní agenturou U.S. GAO (Government Accountability Office). Kongres dále stanovil osm požadavků, jejichž splněním podmiňoval povolení použití systému k jiným účelům než testování.

U.S. GAO posléze shledala, že z osmi požadavků vznesených Kongresem na systém CAPPS II splnila TSA pouze jeden, že vývoj systému je opožděn a že TSA narazila na zásadní překážky v jeho testování (zejména Evropská unie a letecké společnosti

nebyly ochotny poskytnout všechna potřebná data z důvodu ochrany osobních údajů). Dalším závažným nedostatkem systému, na nějž GAO upozornila, byla možnost jeho překonání teroristy, pokud by se jim podařilo vzít na sebe identitu bezúhonných osob.

Program byl proto v polovici roku 2004 ukončen.

2.1.5 Secure Flight a další současné programy

Krátce po zastavení programu CAPPS II oznámila TSA přípravu nového prescreeningového programu Secure Flight, který zčásti staví na dobrých i špatných zkušenostech z předchozích programů a připomínkách k nim, zčásti i na doporučení vyšetřovací komise útoků z 11. září 2001, aby jména cestujících byla porovnávána se seznamy teroristů spravovanými vládou USA, které budou navíc rozsáhlejší než seznamy užívané CAPPS II. Program Secure Flight je vyvinut Ministerstvem vnitřní bezpečnosti USA (Department of Homeland Security, DHS), do jeho přípravy byla rovněž zapojena výše zmíněná agentura GAO.

Secure Flight se vztahuje na lety z, do, nebo uvnitř USA, na lety U. S. leteckých společností mimo území USA a na lety přelétávajícími nad územím USA (vyjma území států Aljaška a Havaj). Jeho implementace byla u vybraných leteckých společností zahájena počátkem roku 2009, plně dokončena u všech leteckých společností pak byla v prosinci 2010.

Hlavní zaměření programu Secure Flight, které má zajistit zlepšení prescreeningu oproti předchozím programům, je následující:

- odstranění nesrovnalosti v původních postupech porovnávání dat cestujících se seznamy nebezpečných osob
- redukce počtu osob, které jsou chybně uvedeny na seznamech No-fly a Selectee
- snížení rizika úniku či neoprávněného vyzrazení informací ze seznamů nebezpečných osob

- integrace informací

Jak bylo právě naznačeno, program tedy funguje opět na principu porovnávání údajů pasažérů se seznamy nebezpečných osob („No Fly" a „Selectee"). Před zavedením Secure Flight byly za tento proces zodpovědné jednotlivé letecké společnosti, s jeho zavedením tato zodpovědnost přešla na TSA. Letecké společnosti jí za účelem porovnání poskytnou o pasažérech následující údaje (označované jako Secure Flight Passenger Data – SFPD):

- jméno a příjmení
- datum narození
- pohlaví
- číslo a zemi vydání pasu (pokud je letecká společnost zjišťuje)
- Redress Control Number (pokud jím pasažér disponuje, viz níže)
- Known Traveler Number / PASS ID (dtto)

Tato data jsou součástí jak PNR, tak datového souboru API, což je Advanced Passenger Information spravovaný Úřadem pro cla a ochranu hranic USA (CBP). V systému APIS (Advanced Passenger Information System) jsou vedeni pasažéři využívající mezinárodní lety. PNR data jsou uchovávána sedm let v aktivním souboru a dalších 8 let v archivu.

Výsledek porovnání zašle TSA letecké společnosti a ta na jeho základě vydá či nevydá cestujícímu palubní vstupenku, případně jej zařadí mezi pasažéry podstupující důkladnější prohlídku.

Algoritmus, jímž Secure Flight posuzuje cestující, je neveřejný. Je ovšem známo, že cestující, kteří cestují častěji, jsou považováni za méně rizikové, tím spíše, pokud cestují pravidelně využívajíce stále stejné linky.

S programem Secure Flight jsou spojeny dva nástroje, které dále zefektivňují screening a prescreening: DHS Traveler Redress Inquiry Program a TSA Pre✓™.

DHS Traveler Redress Inquiry Program

Tento program provozuje, jak je zřejmé z jeho názvu, Ministerstvo vnitřní bezpečnosti (DHS) USA. Často je zkráceně označován jako DHS TRIP. Jeho posláním je řešit případy cestujících, kteří se cítí poškozeni programem Secure Flight, tj. nebyli vpuštěni na palubu či byli při odbavení zdržováni. Tyto osoby mají možnost vyplnit na internetových stránkách Ministerstva vnitřní bezpečnosti[1] formulář, kde uvedou, kterým konkrétním problémům během odbavení čelily. Jejich případ je následně přezkoumán příslušnými úřady. Na základě výsledků tohoto zkoumání jsou aktualizovány či opraveny všechny relevantní záznamy.

Podle statistik DHS se na seznamech potencionálních teroristů vyskytuje méně než jedno procento žadatelů DHS TRIP. Nejčastější příčiny podnětů jsou dvě:

- cestující byl zdržen z jiného důvodu, který nemá souvislost s programem Secure Flight, byl podroben namátkové podrobnější prohlídce, apod.
- jméno, případně jiné údaje cestujícího se podobají údajům některé osoby ze seznamu podezřelých osob

Každé žádosti o přezkoumání v rámci DHS TRIP je přiděleno unikátní sedmimístné číslo, Redress Control Number (často se užívá i zjednodušený pojem redress number). Krom toho, že díky němu může cestující sledovat stav svého podnětu během jeho vyřizování, je zde ještě jedna podstatnější výhoda: cestující může toto číslo uvést během následujících rezervací letenek, což umožní jeho okamžitou a jednoznačnou identifikaci a usnadní proces porovnávání. Výsledkem je další zefektivnění prescreeningu.

[1] https://trip.dhs.gov/

Trusted Traveler

Ministerstvo vnitřní bezpečnosti USA provozuje v rámci ochrany hranic USA několik „Trusted Traveler“[2] programů, majících za cíl umožnit prověřeným a důvěryhodným osobám rychlejší průchod bezpečnostními procedurami.

Jedná se o programy SENTRI, NEXUS, Global Entry a TSA Pre✓™. Program SENTRI je zaměřen především na pozemní cestování mezi USA a Mexikem, proto se jím vůbec nebudeme v této práci zabývat. Podobně nemá valného smyslu podrobně popisovat programy NEXUS (pro cestování mezi USA a Kanadou) a Global Entry (usnadňující celní a imigrační kontrolu při návratu do USA). Zastavíme se však u programu TSA Pre✓™.

Společným rysem zmíněných Trusted Traveler programů je, že zájemci, kteří se přihlásí, se dobrovolně podrobí zkoumání svých osobních údajů a své historie. Jsou-li shledáni nízkorizikovými, obdrží unikátní členské číslo PASS ID. V případě, že jsou občany USA (nebo občany Kanady a zároveň členy NEXUS), mohou toto číslo uvést během rezervace letenky do pole určeného pro Known Traveler Number. Tím se zařadí do programu TSA Pre✓™.

[2] „důvěryhodný cestující“

Obr. 2 – Zadání Known Traveler Number;

Zdroj: [27]

TSA Pre✓™

Program TSA Pre✓™ (precheck) je (pre)screeningový nástroj umožňující „nízkorizikovým" občanům a trvalým obyvatelům USA a Kanady rychlejší absolvování bezpečnostní prohlídky na některých US letištích. V případně příznivého výsledku prescreeningu je cestujícímu vytištěno na palubní vstupenku logo TSA Pre✓™ a cestující může využít zvláštní frontu a stanoviště bezpečnostní prohlídky, která má oproti současné běžné bezpečnostní prohlídce mírnější průběh: cestující si nemusí zouvat boty, sundávat pásek, svlékat kabát (pokud nejde o těžký zimní kabát či bundu). Nemusí také vytahovat přenosný počítač ani sáček s kapalnými látkami (3-1-1

compilant bag[3]) z kabinového (příručního) zavazadla (na restrikcích ohledně množství a způsobu zabalení kapalných látek se však nic nemění).

TSA Pre✓™ tak umožňuje nejen rychlejší průchod nízkorizikových cestujících, ale také úsporu pracovního vytížení zaměstnanců provádějících bezpečnostní prohlídky (screening), kteří se tak mohou důkladněji věnovat cestujícím, kteří nejsou považováni za nízkorizikové. Podle vyjádření šéfa TSA Johna Pistole v Senátu USA v dubnu 2014 využívalo rychlejšího screeningu TSA Pre✓™ cca 40 % cestujících. Cílem je zvýšit tento podíl na 50 % do konce roku 2014 [9].

V současnosti je zapojeno 120 letišť a jedenáct leteckých společností (Air Canada, Alaska Airlines, American Airlines, Delta Air Lines, Hawaiian Airlines, JetBlue Airways, Southwest Airlines, Sun Country Airlines, United Airlines, US Airways a Virgin America).

Jak už bylo uvedeno, do programu TSA Pre✓™ se cestující může zařadit vyplněním svého Known Traveler Number (KTN) do příslušného pole během rezervace letenky. KTN disponují účastníci Trusted Traveler programů zmíněných výše. Ti z občanů a rezidentů USA, kteří KTN zatím nemají, se mohou přihlásit přes internetové stránky DHS, kde vyplní základní osobní údaje a zvolí si z nabídky míst, kam se osobně dostaví k dokončení žádosti. Tam se prokáží dokumenty potvrzujícími jejich identitu, poskytnou otisky prstů a zaplatí poplatek 85 USD, který je nevratný. Pokud je žadatel shledán spolehlivým, obdrží KTN přibližně během 2–3 týdnů.

Členové ozbrojených složek USA mohou jako KTN během rezervace letenky uvést číslo svého služebního průkazu a mohou výhod TSA Pre✓™ využívat automaticky. Dalšími osobami oprávněnými využívat TSA Pre✓™ jsou příslušníci určitých

[3] Pravidlo „3-1-1" je uplatňováno pro LAG (kapaliny, aerosoly, gely) v příručních zavazadlech. Číslice 3 vyjadřuje objem 3,4 unce (100 ml) a udává maximální objem jednotlivých balení. Číslice 1 vyjadřují, že všechna balení musí být zabalena v jednom jednolitrovém sáčku a že jeden cestující může přepravovat pouze jeden takový sáček.

důvěryhodných skupin obyvatelstva, jako např. federální soudci či zaměstnanci tajných služeb.

Kromě zmíněných cestujících, kteří disponují KTN nebo jeho ekvivalentem, můžou výhod rychlejšího screeningu v rámci TSA Pre✓™ využívat i další skupiny cestujících:

- vybraní účastníci věrnostních programů zúčastněných (výše vyjmenovaných) leteckých společností;
- cestující vybraní TSA prostřednictvím programu Secure Flight
- cestující vybraní TSA ad hoc na vybraných letištích prostřednictvím tzv. Managed Inclusion.

Managed Inclusion je program testovaný od roku 2013 na letištích Tampa a Indianapolis a postupně rozšiřovaný na další letiště v USA. Využívá cvičených psů a behaviorální analýzy aplikující poznatky získané z dlouholetého psychologického zkoumání objednaného Ministerstvem vnitřní bezpečnosti USA. Pokud ani psi, ani analytici, kteří pozorují cestující čekající ve frontě, nezjistí nic podezřelého, dotyčný může být vyzván, aby vystoupil z řady a přistoupil k automatu, který náhodně rozhodne, bude-li vpuštěn k rychlejšímu či normálnímu screeningu.

Jistá nahodilost je úmyslně včleněna do celého systému TSA Pre✓™, takže cestujícím nikdy není garantováno, že budou moci využít rychlejšího screeningu. Toto opatření může zastrašit osoby s nekalými úmysly.

Kritici programu Managed Inclusion krátce po jeho zavedení upozorňovali na to, že behaviorální analýza je subjektivní a že osoby, které ji provádějí, neobdržely dostatečný trénink. Zatímco druhá část námitky se vztahuje ke konkrétní aplikaci programu a je-li trénink příslušných zaměstnanců skutečně nedostatečný, lze jej doplnit, první částí námitky je třeba se seriosně zabývat, neboť se týká samotné podstaty programu.

2.2 Prescreening v Evropské Unii

Evropská unie po dlouhou dobu neměla v oblasti bezpečnosti letecké dopravy legislativní pravomoci a zodpovědnost za její zajištění měly jednotlivé státy. Teroristické útoky v USA v září 2011 však přiměly Evropskou komisi k zahájení vývoje společných pravidel v rámci Evropské unie. Tato iniciativa vedla k přijetí Nařízení Evropského parlamentu a Rady č. 2320/2002 v prosinci 2002, kterým se stanovila společná pravidla v oblasti bezpečnosti civilního letectví.

V březnu 2008 bylo toto nařízení nahrazeno Nařízením č. 300/2008. Oproti předchozímu Nařízení tento dokument už předpokládá jakýsi prescreening, když v bodě 4.3 článku 4 stanoví, že „Potenciálně nebezpeční cestující se před odletem podrobují odpovídajícím bezpečnostním opatřením."

Začátky zavádění prescreeningu v EU nebyly jednoduché, oproti USA je vývoj poněkud opožděn. V roce 2006 už byl v USA prescreening s využitím PNR dat běžnou praxí. V květnu 2006 však Evropský soudní dvůr (nyní Soudní dvůr Evropské unie) rozhodl ve prospěch návrhu Evropského parlamentu na anulaci dohody mezi Evropskou komisí a Custom and Border Protection USA (CBP) o sdílení PNR dat cestujících na transatlantických linkách z Evropy. Evropský soudní dvůr nařídil zastavení poskytování těchto dat do 30. září 2006. Pokud by se nepodařilo během léta 2006 dospět k nové dohodě, bylo by cestování mezi EU a USA ohroženo. Postupně však několika dočasných dohod a v červenci 2007 i trvalého ujednání dosaženo bylo, z hlediska ochrany osobních údajů však navzdory rozhodnutí Evropského soudního dvora k žádné významnější změně nedošlo, přestože rozsah údajů o cestujících do USA, které CBP v rámci PNR od leteckých dopravců dostává, byl snížen z 34 na 19 položek.

Výše uvedená fakta se týkají cestujících z EU do USA a striktně vzato souvisí spíše s prescreeningovým systémem USA. Státy Evropské unie zatím nemají a s největší pravděpodobností ani nebudou mít vlastní systém, ale zapojí se do bezpečnostního programu **Next generation screening** (NGen) připravovaného ICAO, IATA, ACI (Airports Council International) a ICCAIA (International Coordinating Council of

Aerospace Industries Associations). Byl představen na konferenci v Montrealu v září 2012.

Vývoj programu koordinuje ICAO Technical Advisory Group on Next generation screening (ICAO TAG NGen). Plán schválený na konferenci v Montrealu předpokládá, že se program postupně rozvine do roku 2020, přičemž bude využívat následujících prostředků:

Údaje o cestujících

Základním zdrojem pro analýzu údajů o cestujících budou již existující databáze – PNR, API a informace získané při check-in. Za vyhodnocení těchto dat (stanovení rizika) můžou být zodpovědné vládní organizace nebo letecké společnosti, případně mohou tyto subjekty spolupracovat.

Ve střednědobém horizontu (rok 2017) NGen počítá s ustanovením „National Targeting Centres" zaměřujících se na monitorování rizikových osob v dalších státech (v červnu 2014 bylo založeno v Austrálii, dále fungují např. v USA, Kanadě, UK).

V dlouhodobém horizontu (od roku 2020) je plánována užší mezinárodní či globální spolupráce zmíněných národních center, sdílení dat, uzavření multilaterálních dohod.

Known Traveler

Zde jde o obdobu stejnojmenného programu užívaného v USA, o němž bylo pojednáno výše. Vládním organizacím má být umožněno provést detailní bezpečnostní prověrku osob, které o ni dobrovolně požádají. Podle plánu NGen přitom mohou jednotlivé státy přihlédnout k prověrkám, které žadatelé podstoupili dříve či udělit členství v programu Known Traveler určitým osobám, např. členům ozbrojených složek apod., automaticky.

Ve střednědobém horizontu se počítá s uzavíráním dvoustranných dohod mezi jednotlivými státy, které by vzájemně uznávaly výsledky ohodnocení rizik, v dlouhodobém horizontu pak s jejich uznáváním na širší mezinárodní úrovni.

Ověřování identity

V této oblasti schválený plán předpokládá shromažďování biometrických údajů za účelem zvýšení spolehlivosti identifikace pasažérů, její automatizaci a v dlouhodobém horizontu použití pasů s integrovaným čipem (e-passports).

Behaviorální analýza

Behaviorální analýza je považována za doplňkovou součást posuzování rizika a může být užita buď ve spojení s ostatními komponenty, nebo samostatně. Může nabývat různých forem, od osobního dotazování až k pozorování pasažérů pohybujících se na letišti bez jejich vědomí.

Alternativní přístupy

Mezi alternativní přístupy zajištění bezpečnosti, s nimiž počítá NGen, se řadí například náhodný výběr cestujících k rozsáhlejšímu screeningu, použití cvičeních psů k odhalování výbušnin, apod.

ICAO TAG NGen vybízí členské státy ICAO jednak k přijetí takových zákonů, které by umožnily implementaci navrhovaných inovací, jednak k průběžnému sdílení zkušeností jednak mezi státy a ICAO, tak mezi státy a průmyslovým sektorem, který se na vývoji NGen podílí.

2.3 Prescreening v Izraeli

Politicko-bezpečnostní situace v Izraeli je napjatá prakticky nepřetržitě od vzniku tohoto státu v roce 1948. Z tohoto důvodu mají jeho bezpečnostní složky dlouholeté zkušenosti a i prescreening cestujících v letecké dopravě má v Izraeli mnohem delší tradici než v USA, tím spíše mnohem delší než v Evropě.

Zatímco po teroristických útocích v roce 2001 došlo v USA ke zpřísnění bezpečnostních opatření, které by se dalo označit jako plošné a teprve postupně probíhalo zavádění prescreeningu a profilingu, kdy k pasažérům není a priori přistupováno jakožto ke stejně rizikovým, v Izraeli využívají profilingu už několik desítek let.

Velmi významnou součástí bezpečnostní kontroly na letištích v Izraeli je behaviorální analýza cestujících, jež zde byla uvedena do praxe už roku 1970. Je založena především na rozhovorech specializovaných pracovníků letiště se všemi cestujícími bez výjimky. Během rozhovorů tito pracovníci sledují u prověřovaných cestujících obsah i konzistenci odpovědí, řeč těla, způsob jejich reakcí atd. Zpozorují-li něco podezřelého, rozsah rozhovoru se může rozšířit nad obvyklou úroveň nebo je zahájen další rozhovor s jiným bezpečnostním pracovníkem. Pokud pochybnosti o důvěryhodnosti cestujícího přetrvávají, podrobí jej pracovníci letiště mnohem přísnějšímu screeningu, který může trvat i desítky minut až jednotky hodin. Cestujících zařazených k podstoupení rozsáhlejší bezpečnostní prohlídky je v praxi 2–5 %.

Metodika těchto rozhovorů je pochopitelně neveřejná. Z veřejných zdrojů je známo, že se pracovníci dotazují například na jména osob, s nimiž se dotyčný v Izraeli setkal, s nimiž si vyměňoval kontaktní informace, chtějí předložit pozvánku na událost, kvůli níž dotyčný cestuje, prohlíží si digitální fotografie pořízené cestujícím a podobně. [17]

Zdá se, že jde o účinný způsob zajištění bezpečnosti, neboť na nejvytíženějším izraelském letišti v Tel Avivu nedošlo k selhání bezpečnostních kontrol (ve smyslu, že by přes ně pronikl terorista) od roku 1972. I přesto, že cestující nejsou nuceni se zouvat ani vzdát se svých láhví s nápoji.

3 Technologie pro získávání informací

V této kapitole se zaměřím na některé technologie vyvíjené v rámci projektu INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment), který je od roku 2009 s rozpočtem převyšujícím 14,8 milionů Eur financován Evropskou unií. Pokusím se tyto technologie stručně popsat a analyzovat, zda by bylo možné je využít i pro prescreening.

INDECT má být inteligentní monitorovací a vyhodnocovací systém, který má automaticky detekovat hrozby trestných činů a abnormálního chování prostřednictvím kamerových systémů, dolováním dat z informací získaných z veřejně přístupné části internetu a sledování pohybu mobilních telefonů prostřednictvím GPS a GSM.

Na projektu se podílí několik evropských univerzit, mimo jiné i Vysoká škola báňská – Technická univerzita Ostrava.

Systém má být propojen s databází údajů v biometrických pasech, a tak bude schopen identifikovat osoby na základě vizuálního záznamu jejich obličeje, příp. dalších biologických charakteristik jedince. Primárním uživatelem systému má být policie. Prescreening není zamýšlen přímo jako účel systému.

3.1 Monitorování fyzických objektů a detekce hrozeb

Pro monitorování fyzických objektů (především osob) plánuje INDECT využívat stávající kamerové systémy (CCTV). Oficiální internetová prezentace projektu prohlašuje:

„Současné CCTV monitorovací systémy jsou převážně založeny na přístupu stálého sledování, kde je sledovaná oblast pod nepřetržitým dohledem operátora. Je-li operátor nečestný, může to vést k zneužití soukromí.“ [18]

INDECT má být naproti tomu založen na monitorování hrozeb (také známo jako „black/dark screen monitoring“), kde se systém zaměřuje na potencionálně

nebezpečné situace, které má automaticky detekovat, a umožní operátorovi přístup k videu jen tehdy, kdy je jeho pozornost momentálně potřebná. Operátor pak vyhodnotí, zda se skutečně jedná o nebezpečnou situaci a rozhodne o případných opatřeních.

3.1.1 Detekce nebezpečných situací na základě parametrického modelu

Automatická detekce událostí ve zvukových a obrazových datech obdržených z kamer vyžaduje celou řadu procesních úkonů. Nejdůležitějšími fázemi jsou: detekce objektu, parametrizace objektu, klasifikace objektu, analýza interakcí mezi objekty a konečně rozpoznání události.

Situací se rozumí interakce mezi objekty.

Změny objevivší se v analyzovaných parametrech lze považovat za akce, společně se vyskytující akce u několika objektů za interakce. Za účelem sledování určitých situací lze vytvořit interakční model.

Detekce objektu

Pro detekci objektu je možno použít různé algoritmy a metody. Jako nejefektivnější se ukázala diferenční metoda, jejíž implementace je relativně jednoduchá a nemá přehnané hardwarové nároky. Její algoritmus je založen na porovnání dvou prvků: aktuálního obrazu a referenčního obrazu, který reprezentuje pozadí. Referenční obraz by měl být průběžně přizpůsobován, aby zůstal věrnou reprezentací pozadí, které se může měnit.

Správně konfigurovaný systém s využitím diferenční metody mimo jiné umožňuje:

- detekci zahájení a ukončení pohybu,
- detekci vstupu a výstupu objektu do/z definované oblasti,
- detekci a sledování lidí a vozidel,
- signalizaci opuštěných objektů,

– detekci davu atd.

Parametrizace a klasifikace objektu

V dalším kroku se objektům přiřadí parametry jako poloha, velikost, rychlost, vzhled, tvar apod. Pokud je objektem osoba, sledují se biometrické charakteristiky – obličej, duhovka, tvar ucha, ruky atd.

Objekty jsou pak podle parametrů klasifikovány do čtyř hlavních kategorií: osoby (dospělí, děti), vozidla, ostatní pohybující se objekty (např. zvířata), nepohyblivé objekty (např. zavazadla).

Přesnost analýzy objektu se zvyšuje zapojením analýzy zvuku. Nebezpečné a nelegální jednání bývá často doprovázeno výskytem charakteristických zvuků (křik, volání o pomoc, rozbité sklo apod.). Ne vždy je však možno přiřadit detekovaný zvuk konkrétnímu objektu.

Analýza interakcí mezi objekty

Interakce můžeme rozdělit na dva základní typy:

– mezi objektem a pozadím (neovlivňující jiné objekty)

– mezi objektem a jinými objekty

Pokud jde o jednotlivé objekty, lze definovat modely pro vstup nebo výstup objektu do/z definovaného prostoru či překročení bariéry, ať už fyzické nebo virtuální.

Pro objekty – osoby je možné definovat další akce (mávání rukou, sedění, ležení) založené na změně tvaru objektu a vzdálenostech hraničních bodů tohoto objektu.

Základní modelové situace pro jednotlivé objekty uvádí tabulka:

Parametr	**Možné situace**
Poloha	Objevení se, zmizení; uvnitř oblasti či na její hranici
Pohyb	Vstup do oblasti, výstup z oblasti, překročení hranice; správný či nesprávný směr pohybu
Rychlost	Zvýšení či snížení rychlosti
Akce osob	Mávání, sedění, ležení
Zvuk	Exploze, výstřel, křik, rozbité sklo

Tab. 1

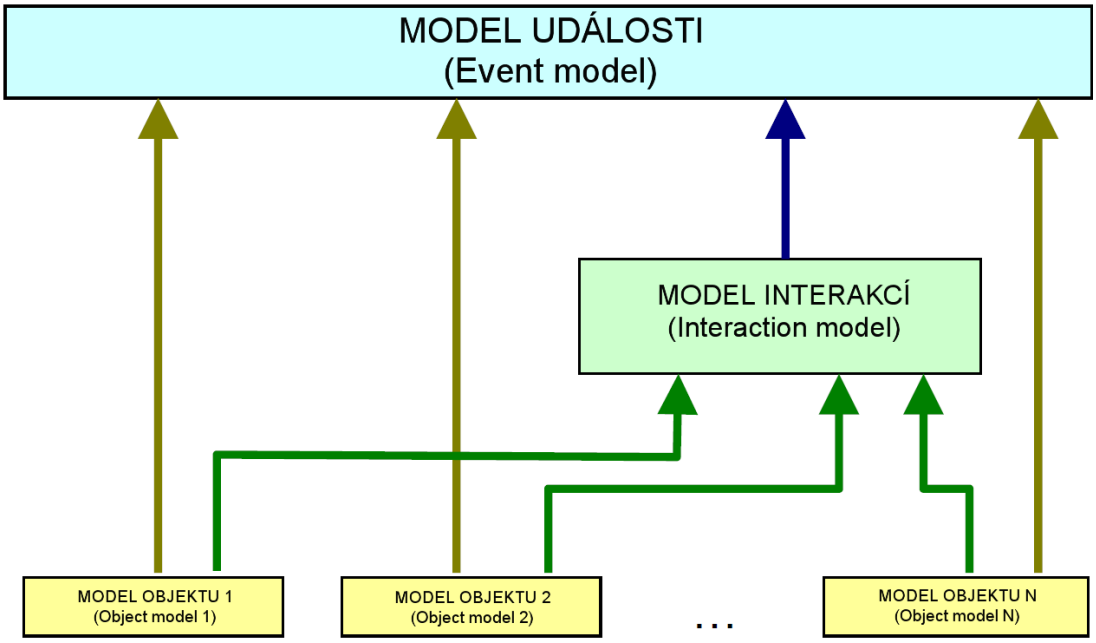
Pokud jde o interakce mezi více objekty navzájem, INDECT je zaměřen převážně na:

- interakce mezi osobami a vozidly (nastoupení do auta, vystoupení z auta, kolize s jedoucím autem)
- interakce mezi osobami a předměty (opuštění předmětu, zanechání předmětu na místě, zahození objektu, překonání překážky)
- analýzu davu.

Rozpoznání události

Událost je definována jako činnost vykonaná jedním nebo více objekty. Rozpoznání události je založeno jednak na vzájemném působení činností provedených jednotlivými objekty, jednak na vzájemném působení mezi objekty jinými objekty nebo statickým pozadím.

Objekt modelu poskytuje data ohledně stavu každého objektu analyzovaného ve videu, například informace o jeho pozici, velikosti, vzhledu, pohybu atd. Model interakcí poskytuje informace o vztazích mezi modelovanými objekty a ostatními objekty a pozadím. Tyto modely však ještě neposkytují interpretaci činnosti prováděné objekty. Proto je vytvořen model události.



Obr. 3 – Geneze modelu události, zdroj: [25]

Model události zpracovává data obdržená z modelů objektů a interakcí a posuzuje, zda jsou podmínky, jimiž je událost definována, splněny. Model události není omezen na jeden zdroj dat a na interpretaci pouze aktuálně probíhajících dějů, ale ukládá historii stavu objektů (z modelů objektů), detekovaných interakcí (z modelu interakcí) i dříve detekovaných událostí. To má dva přínosy – filtraci momentálních událostí (např. objektu detekovaného v omezené oblasti po velmi krátký čas) a detekci událostí popsaných jako řetězec časově oddělených úkonů.

Samotné vyhodnocování události probíhá na základě posuzování splnění definovaných podmínek. Příkladem budiž situace opuštění zavazadla na letišti: objekt typu „osoba" musí opustit objekt typu „zavazadlo", odejít od něj na definovanou vzdálenost a nevrátit se do jeho blízkosti během definované doby. Podobně lze definovat sérii snadno zhodnotitelných podmínek i pro další relativně složité situace, které mohou nastat.

Využití v prescreeningu

Právě popsaná součást systému INDECT má především identifikovat situace jako je např. krádež předmětu, zanechání předmětu na místě, vstup do zakázaného prostoru, přepadení, souboj dvou osob apod. S účelem prescreeningu se tedy do značné míry míjí a pro prescreening bude ve své současné podobě asi jen stěží využitelná. Není totiž známo, že by se kdy například teroristé před únosem letadla pokusili na sebe upoutat pozornost tím, že by někoho přepadli na letišti.

Pokud se dá věřit informacím uvedeným v populárním časopise Der Spiegel (ze serióznějších zdrojů se je ověřit ani vyvrátit nepodařilo, což není vzhledem k povaze těchto informací překvapivé), je empiricky zjištěno, že „teroristé bývají nervózní, pospíchají a téměř nikdy se nezastaví na kávu." [19] Pokud bude v této oblasti proveden nějaký seriosní výzkum, který by ukázal, že je možné hodnotit rizikovost cestujících na základě jejich fyzických projevů zaznamenatelných touto technologií, bude možné ji využít i pro prescreening.

Tato technologie však může být dobrým nástrojem alespoň v oblasti letištní bezpečnosti, zvláště pokud jde o identifikaci opuštění zavazadla, kde může být výbušnina apod. Technologie jistě bude dále vyvíjena a je možné, že na způsoby, jak může být užitečná, se teprve přijde. Autoři sami předpokládají, že bude možné s pomocí této technologie identifikovat například vytažení střelné zbraně zpod kabátu a zamíření.

3.2 Monitorování počítačových sítí a detekce hrozeb

V rámci systému INDECT jsou také vyvíjeny technologie, jež mají za cíl analyzovat nestrukturovaná data vyskytující se v počítačových sítích, zvláště internetu, za účelem prevence kriminality. Vzhledem k tématu této práce (prescreening) prozkoumáme možnost využití technologií umožňujících zjišťování vztahů mezi osobami a organizacemi a odhalování potencionálně nebezpečných internetových stránek.

3.2.1 Zjišťování vztahů a vazeb mezi osobami a organizacemi

Za účelem využití potenciálu, jenž se nachází v obrovském množství informací obsažených na internetu, byla vyvinuta technologie umožňující automatickou extrakci obsahu z běžného jazyka. INDECT zde navazuje na projekt Automatic Content Extraction (ACE) [20], který umožňuje automatické zpracování dat z různých zdrojů (internetové stránky, blogy, sociální sítě) a jejich následnou klasifikaci a filtraci.

Konkrétně je cílem projektu ACE získat z běžného jazyka (přičemž se neomezuje na zdroje v textové formě, ale i zpracovává i data obrazová a zvuková) následující:

- entity zmiňované v textu
- vztahy existující mezi identifikovanými entitami
- události, jichž se identifikované entity účastní
- všechny odkazy na entity a jejich vlastnosti

Na základě právě zmíněného je ACE rozdělen na následující čtyři oblasti:

- Entity Detection & Tracking (EDT): Cílem EDT je rozpoznání entit a jejich přiřazení k jednomu z následujících typů: osoby či skupiny osob, organizace, místa, objekty občanské vybavenosti, geografické / sociální / politické, dopravní prostředky a zbraně.
- Relation Detection & Characterization (RDC): Cílem je identifikovat vztahy mezi dvěma entitami identifikovanými v předchozím kroku (EDT) a přiřadit tyto vztahy k jednomu z následujících typů: fyzický vztah, osobní / společenský vztah, vztah mezi disponentem a majetkem, ostatní vztahy (příslušnost k etnickým a náboženským skupinám)
- Event Detection & Characterization (EDC): Cílem je identifikovat události a přiřadit je k jednomu z pěti definovaných typů: zničení / poškození / zabití, vytvoření / vylepšení, pohyb / změna sídla apod., přesun vlastnictví nebo kontroly, interakce mezi osobami a organizacemi

- Entity Linking Tracking (LNK): Cílem je shromáždit všechny odkazy na entity a jejich vlastnosti.

ACE je schopen analyzovat data v angličtině, čínštině a arabštině a je považován za silný nástroj pro identifikaci a třídění entit a objevování vztahů a událostí, v nichž identifikované entity participují. Jeho nevýhodou však je, že není snadno rozšiřitelný a modifikovatelný, neboť postrádá znalostní bázi a schopnost modelovat strukturované vztahy. Tyto nevýhody překonává Knowledge Based Population (KBP), který využívá k posuzování zjištěných entit znalostní báze z „infoboxů" internetové encyklopedie Wikipedia, což se ovšem také neobejde bez problémů, neboť zde není zajištěna plná integrita dat kvůli nejednotnosti v používání pojmů a atributů.

Proto bylo přistoupeno k vývoji nového systému, který by stavěl na silných stránkách ACE a KBP. Zkoumají se nové metody zjišťování vztahů, využívající možnosti různých systémů, jak dozorovaných (supervised), které vyžadují součinnost vyškoleného operátora, tak nedozorovaných (unsupervised).

Poslední publikované informace hovoří o tom, že požadavky INDECTu efektivně splňuje nedozorovaná metoda založená na algoritmech teorie grafů, v nichž uzly tvoří nalezené entity (typologizované do kategorií osoby, organizace, místa) a hrany představují vztahy mezi odpovídajícími entitami. Tato metoda dosahuje úrovní spolehlivosti a přesnosti dozorovaných metod.

Příklad: Máme věty získané z internetu pomocí vyhledávače (bot):

- Josef Novák je ředitel KKC
- Dcera Josefa Nováka, Marie Nováková, byla jmenována do funkce personalistky v KKC

Vytěžovací systém je schopen identifikovat vztah mezi entitou typu OSOBA (Josef Novák) a entitou typu ORGANIZACE (KKC). Tento konkrétní vztah může být označen jako vztah typu ZAMĚSTNÁNÍ. Stejný vztah existuje i mezi entitami téhož typu ve druhém příkladu, navíc lze z druhé věty zjistit ještě další typ vztahu, totiž PŘÍBUZENSTVÍ.

Využití v prescreeningu

Možnost využití Relation Extraction (RE), tedy zjišťování (či dolování) vztahů mezi osobami a organizacemi, v prescreeningu vypadá poměrně slibně.

Při vhodné implementaci bude možné zkoumat v rámci prescreeningu nejen osoby vyskytující se přímo na existujících watchlistech a seznamech potencionálně nebezpečných osob, ale i osoby, které mají na tyto osoby vazby zjištěné zde alespoň stručně naznačenou metodou.

3.2.2 Odhalování potencionálně nebezpečných internetových stránek

Součástí systému INDECT jsou také technologie pro identifikaci potencionálně nebezpečných či podezřelých internetových stránek za účelem monitoringu a predikce kriminálních aktivit.

„Podezřelou internetovou stránkou" se zde rozumí jakákoliv internetová stránka, která svým obsahem zjevně porušuje zákon, nebo je z toho podezřelá. Může jí být například stránka, která nabádá k násilí, podvodům, financování terorismu či jiných zločinů. Prostřednictvím internetu lze též pořádat nábory nových členů teroristických organizací.

Metoda detekce podezřelých internetových stránek se skládá z následujících kroků:

1. **Pre-processing** – Vstupní text je rozčleněn na jednotlivé tokeny (slova), které jsou následně lemmatizovány (lemma je slovníkový tvar slova – např. lemma pojmů „obchodě" a „obchodem" je obchod). Poté jsou odfiltrována předdefinovaná neužitečná slova (stop words), jako nejčastěji spojky či předložky, které se vyskytují ve všech typech dokumentů a nejsou nositeli speciálního významu.
2. **Pattern Generation** – Jelikož jednotlivá slova (lemmata) můžou nést více významů současně (tím spíše v kriminálním prostředí, kde je užíván tzv. argot), k posouzení významu nestačí používat jednotlivá slova, ale n-slovné

kombinace slov (N-grams); čím vyšší je hodnota n, tím přesněji je definován význam, ale zároveň se snižuje pravděpodobnost nalezení stejné fráze v jiném textu, což znesnadňuje porovnání.

3. **Pattern matching** – Tento modul porovná patterny, které se vyskytují na internetových stránkách dříve označených za podezřelé s patterny vyskytujícími se na tzv. normálních stránkách, a vygeneruje patterny typické pro podezřelé stránky, které jsou označeny jako „initial patterns" a uloženy do databáze.

4. **Link Module** – „Initial patterns" vygenerované v předchozím modulu jsou použity jako vstup pro vyhledávač (search engine), který vygeneruje další odkazy na podezřelé stránky.

5. **Crawler** – Web crawler je „robot", jehož cílem je následovat URL odkazy vedoucí z podezřelých stránek a vytvořit databázi internetových stránek, na něž je odkazováno.

6. **Pre-Processing** – Nový obsah nalezený crawlerem je zpracován stejným způsobem jako v prvním kroku.

7. **Pattern generation** – z nového podezřelého obsahu jsou vygenerovány nové patterny jako v kroku č. 2.

8. **Pattern Matching** – Tento modul porovná nové patterny nového podezřelého obsahu (č. 7) s patterny extrahovanými z „normálních" stránek (č. 2).

9. **Similarity calculation –** Zde dojde ke kalkulaci podobnosti mezi „initial patterns" (z databáze podezřelého obsahu) a potencionálně podezřelými patterny zjištěnými v č. 8. Výstupem z tohoto modulu je sada patternů označených jako podezřelé.

10. **Website classification** – S využitím podezřelých patternů vygenerovaných v předchozím kroku jsou z databáze stránek vytvořené v č. 5 vybrány vysoce podezřelé stránky.

Tento proces se opakuje stále dokola.

Využití v prescreeningu

I tato technologie může být v prescreeningu prospěšná, i když jistě v poněkud omezenější míře než předchozí pojednaná technologie zjišťování vztahů a vazeb, která pracuje přímo se jmény osob, zatímco tuto technologii je nutno doplnit metodikou zjišťování identity osob, které problematické internetové stránky vytvářejí či v nich nějakým způsobem figurují. Neobejde se tedy bez další zpravodajské práce, ale v případě, že spolupráce se zpravodajskými službami bude navázána a optimálně nastavena, jeví se tato technologie jako relativně snadno využitelná.

3.3 Behaviorální profiling

Behaviorální profiling vychází z poznatku, že u pachatelů kriminálních činů existují obdobné vzorce chování, které lze pozorovat a statisticky hodnotit. Ze zločinů, které se v minulosti odehrály a byly vyšetřeny, se shromáždí data o chování a dalších psychologických charakteristikách jejich pachatelů, která se následně analyzují za účelem vytvoření profilu „typického" pachatele. Ten může mít dvojí využití: jak při vyšetřování, tak při prevenci.

Geografickým profilingem, při němž se z informací zjištěných z dřívějších vyřešených případů zjišťují místa, kde se zvýšenou pravděpodobností dojde ke zločinu, která zločince „přitahují", nebo naopak místa, kde je spáchání zločinu méně pravděpodobné, se tato práce nebude zabývat, neboť potencionální místo činu je předem dané – letiště či letadlo. Zaměříme se spíše na zjišťování charakteristik nebezpečných osob.

INDECT vyvíjí metodiku zjišťování profilu analýzou policejních zpráv o vyšetřených zločinech. V nich se mohou vyskytovat mimo jiné následující informace:

- pohlaví pachatele,
- věk pachatele,

- etnické vzezření pachatele,
- přítomnost nebo absence specifických způsobů jednání,
- popis způsobu spáchání zločinu.

Při vývoji této metody se INDECT zaměřuje zejména na analýzu popisu spáchání zločinu s cílem získat z něj informace o specifických osobních charakteristikách daného zločince. Dalším zdrojem dat mohou být poznámky, emaily a další dokumenty vytvořené například teroristickou organizací.

INDECT svou metodu staví na základech výzkumu R. Bache a kol. [3], který se zaměřil na analýzu věku, pohlaví, rasy a zaměstnání (zaměstnaný/nezaměstnaný) pachatelů a souvislost těchto charakteristik s různými typy kriminálních činů (krádež, krádež v obchodě, krádež z vozidla, loupež, vloupání, přepadení…). R. Bache a kol. (tamtéž) uvádí, že zkoumání lze rozšířit na libovolné jiné charakteristiky pachatelů, které mohou mít nějaký význam, např. užívání drog, vzdálenost z bydliště pachatele na místo činu, kriminální historii pachatele, rodinný stav, apod. Limitující je zde ovšem dostupnost zdrojových dat – tyto charakteristiky musí totiž být nejprve pozorovány a zaznamenány u již vyřešených případů a musí jít o statisticky relevantní vzorek.

Shromážděná data jsou analyzována počítačově. R. Bache a kol. ve zmíněné studii popisuje metodiku této analýzy, zde ji ovšem uvádět nebudu, neboť značně přesahuje rozsah této bakalářské práce. V závěru studie autoři uvádí, že mezi konkrétními kriminálními činy a konkrétními osobnostními charakteristikami skutečně existují korelace. Dá se předpokládat, že pokud se namísto charakteristik typu věk, užijí výše naznačené psychiatrické či kriminalistické charakteristiky, bude úspěšnost tohoto profilingu ještě vyšší.

Předpokládá se, že profily nebudou touto technologií vytvořené neměnně jednou provždy, ale budou průběžně aktualizovány a precizovány, jak budou k dispozici nová data o spáchaných zločinech.

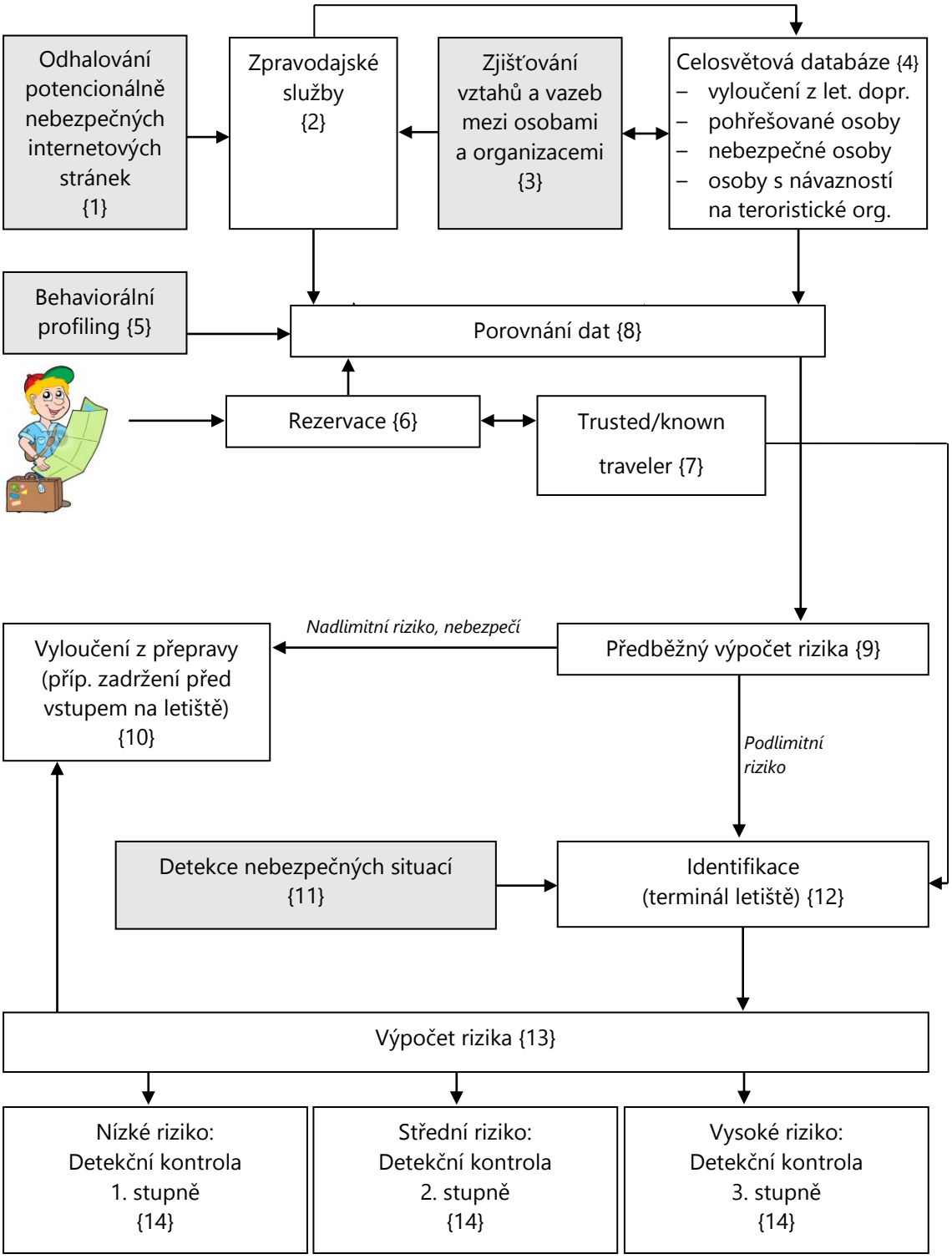
Použití v prescreeningu

Použití této technologie v prescreeningu se jeví jako perspektivní, ovšem spíše až ve vzdálenější budoucnosti. Ač od behaviorálního profilingu nelze očekávat exaktní výsledky a jednoznačné určení pachatele, z dosavadního zkoumání vyplývá, že tato technologie umožní ohodnotit rizikovost cestujících alespoň s určitou přesností v rámci pravděpodobnosti.

Je nesporné, že v případě této technologie musí ještě proběhnout rozsáhlejší výzkum. Jelikož protiprávní činy v letectví nejsou zdaleka tak časté jako například krádeže, největší překážkou nejen v zavádění, ale i samotném zkoumání této technologie je zcela určitě malý vzorek dat, z nichž lze vytvořit profily pachatelů.

4 Model

4.1 Schéma



4.2 Popis

Moderní technologie diskutované v této práci jsou ve schématu označeny šedě.

1. **Odhalování potencionálně nebezpečných internetových stránek**

   Jeden ze vstupů, pro nějž může být využívána technologie popisovaná v kapitole 3.2.2, lze použít nikoli přímo, ale ve spolupráci se zpravodajskými službami, které mají možnost identifikovat osoby figurující za zjištěnými nebezpečnými internetovými stránkami.

2. **Zpravodajské služby**

   Funkce zpravodajských služeb v tomto návrhu je využívat společně s vlastními prostředky technologie {1} a {3} a takto získanými informacemi doplňovat navrhovanou celosvětovou databázi {4}. Zároveň mohou poskytovat data i přímo, bez prostřednictví zmiňované databáze.

3. **Zjišťování vztahů a vazeb mezi osobami a organizacemi**

   Technologie popisovaná v kapitole 3.2.1. Vyhledává podezřelé vazby mezi osobami z databáze {4} a osobami a organizacemi, které v této databázi zatím nejsou. Výsledky předává zpravodajským službám {2} nebo přímo do zmíněné databáze {4}.

4. **Celosvětová databáze**

   Navrhovaný model počítá se zavedením databáze, která by byla celosvětovou obdobou watchlistů používaných v USA a obsahovala by informace o potencionálně nebezpečných osobách, osobách zcela vyloučených z letecké dopravy, osobách spojených s teroristickými organizacemi, pohřešovaných osobách apod.

5. **Behaviorální profiling**

   Technologie popisovaná v kapitole 3.3 by v případě, že se ji podaří dostatečně vyvinout, mohla by být nápomocna při analýze dat {8} a výpočtech rizik {9, 13}.

6. **Rezervace**

   Při rezervaci letenky poskytne cestující své osobní údaje, s nimiž se dále pracuje.

7. **Trusted/known traveler**

   Model počítá se zapojením programů pro důvěryhodné cestující, obdobných programům, jež jsou popisovány v kapitole 2.1.5.

8. **Porovnání dat**

   Cestujícím zadané osobní údaje jsou porovnány se záznamy o nebezpečných nebo naopak důvěryhodných osobách.

9. **Předběžný výpočet rizika**

   Na základě porovnání dat je předběžně vypočteno riziko.

10. **Vyloučení z přepravy (příp. zadržení před vstupem na letiště)**

    Pokud se během výpočtu rizika zjistí, že riziko, které představuje dotyčný člověk je příliš vysoké, nebude mu umožněno odbavení. V případě velmi vysokého rizika je možné jej zadržet dokonce ještě před vstupem na letiště.

11. **Detekce nebezpečných situací**

    Spíše teoreticky je do modelu zařazena i tato položka, kterou lze v současnosti využít pro prescreening jen těžko, ovšem není vyloučeno, že v budoucnu – po jejím zdokonalení a přizpůsobení – tomu bude jinak.

12. **Identifikace (terminál letiště)**

    Počítá se s identifikací cestujícího s využitím biometrických údajů uložených v čipu cestovního dokladu, čímž se totožnost osoby s údaji, které zadala při rezervaci a které byly hodnoceny v rámci prescreeningu, určí s velmi vysokou mírou spolehlivosti.

13. Výpočet rizika

Z informací shromážděných během celého procesu je konečně vypočtena míra rizika představovaná dotyčným cestujícím.

14. Detekční kontrola

Podle výsledku výpočtu rizika podstoupí cestující přísnější, standardní nebo méně přísnou detekční kontrolu.

5 Vyhodnocení navrženého modelu

Model navržený v této bakalářské práci se snaží řešit v současnosti a pravděpodobně i budoucnosti existující problém, jímž je neadekvátní zdržení a snížení komfortu cestujících v letecké dopravě při jejich bezpečnostních prohlídkách. Současný převládající způsob provádění bezpečnostních kontrol se vyznačuje dvěma rysy:

1. ke všem cestujícím je přistupováno stejně (detekční kontrola je stejně důkladná),
2. bezpečnostní kontrola spočívá ve snaze odhalit předměty, jimiž může být spáchán protiprávní čin.

Řešením neefektivity tohoto přístupu je prescreening, který se místo nebezpečných předmětů zaměřuje na analýzu osob, které tyto předměty mohou použít (ad 2) a s jehož pomocí lze cestující rozdělit do kategorií, podle zjištěné míry rizika představovaného tím kterým cestujícím (ad 1). Cestující, kteří budou shledáni jako téměř bezrizikoví, nebudou muset podstupovat tak důkladnou detekční kontrolu jako ti, u nichž byla zjištěna míra rizika vyšší. Konkrétní náplň jednotlivých stupňů detekční kontroly a možnosti využití nových technologií v této oblasti by měly být předmětem dalšího výzkumu.

Jak už bylo diskutováno u jednotlivých technologií ve 3. kapitole této práce, pokud budeme posuzovat poměr jejich přínosu vůči úsilí vynaloženému při jejich zavádění jakožto součástí procesu prescreeningu, ne všechny se už na druhý pohled ukázaly jako stejně vhodné a efektivní.

U těch, jež se jeví jako efektivnější (Odhalování potencionálně nebezpečných internetových stránek a Zjišťování vztahů a vazeb mezi osobami a organizacemi) jejich použití poněkud komplikuje fakt, že budou pravděpodobně muset být provozovány ve spolupráci se zpravodajskými službami, což samo osobě znamená, že už i legislativní zakotvení projektu bude náročné. Další skutečností ukazující na to, že

přijetí potřebné legislativy nebude vůbec jednoduché, je to, že jde o mezinárodní či dokonce globální projekt.

Technologie Detekce nebezpečných situací a Behaviorální profiling se mi jeví pro použití v prescreeningu v současnosti jako méně efektivní, ovšem každá z jiného důvodu. První zmíněná technologie na současném stupni vývoje zatím neumožňuje posuzování psychologických charakteristik na základě tělesných pohybů osob zaznamenaných kamerami, i když tento potenciál nejspíš má a její použití pro analýzu řeči těla v budoucnosti není vyloučeno. Uplatnění behaviorálního profilingu zase troskotá na skutečnosti, že nedisponujeme dostatečným a statisticky významným vzorkem dat, z něhož by bylo možné vytvořit obecně využitelné profily typických pachatelů protiprávních činů proti letecké dopravě.

Za dobrý prvek v modelu považuji obdobu už v současnosti v USA využívaného konceptu Trusted traveler. Pozitivní na něm je, že cestující se nechává prověřit a nahlédnout do svého soukromí vědomě a dobrovolně.

Z praktického hlediska, ať už při zavádění nebo při provozu, se mi jeví jako nejvhodnější, aby byla navrhovaná databáze {4} i proces porovnávání dat {8} pod záštitou ICAO. To může asi nejsnáze zabezpečit prosaditelnost tohoto pojetí i důvěryhodnost systému.

Pokud jde o další technologie, které by mohly být využitelné, na pomezí screeningu a prescreeningu by zřejmě nebylo marné pokusit se prozkoumat možnost automatizace rozhovorů, jakých se užívá během bezpečnostních kontrol na letištích v Izraeli. Vyhodnocování by mohlo fungovat obdobně jako v případě detektorů lži, kdy by se sledovaly fyzické reakce na položené otázky, jako například změna tělesné teploty, odporu, tepové frekvence apod. Tento námět může být předmětem dalšího výzkumu, stejně jako konkrétní algoritmus výpočtu rizikovosti ze vstupních dat a další náležitosti, které přesahují rámec této práce.

Ochrana soukromí

Mnoho lidí si nepřipouští možnost příchodu totalitního režimu v blízké budoucnosti, řekněme v horizontu desetiletí. Tento postoj nesdílím. Lidská přirozenost se nemění, a tak přesvědčení, že nyní je lidstvo „dál" a žádná další totalita tudíž nehrozí (což si lidé mysleli vždycky), nelze označit jinak než za naivní.

Potíž je v tom, že se současnými technologiemi by případný totalitní režim měl mnohem snadnější kontrolu nad rozsáhlými oblastmi života jedinců i rodin a tak by se pravděpodobně jednalo o režim ještě horší, než ty předešlé. Pochybnosti nerozptyluje ani fakt, s níž jsem se při studiu literatury během psaní této práce mnohokrát setkal, a sice že byla deklarována snaha přesvědčit veřejnost, aby navrhované změny, znamenající zvýšení intenzity sledování soukromých záležitostí občanů, akceptovala. Možná to ukazuje na to, že spíše než sami občané si tato opatření žádají představitelé sociálně-inženýrských zájmů…

Jistě, existují snahy o ochranu osobních údajů před zneužitím, ty ovšem většinou předpokládají, že tyto údaje či informace budou zneužity zvenčí. Co když je však zneužije jejich správce – stát? Přiznávám, že nemám ponětí, jak tomu předejít. Pokládal jsem však za nutné na to zde závěrem alespoň upozornit.

Závěr

Cílem mé bakalářské práce bylo popsat přístupy k prescreeningu v zemích, kde je už užíván, prozkoumat možnosti jejich vylepšení zapojením moderních technologií a na tomto základě navrhnout model fungování prescreeningového systému.

Na začátku práce jsem nejprve uvedl přehled historie letecké kriminality, z něhož plyne, že v drtivé většině případů jsou zločiny páchány s využitím předmětů donesených pachatelem na palubu. Obrana spočívá prakticky především v detekci těchto předmětů a zabránění jejich vnesení na palubu. Slabým místem tohoto přístupu je jednak to, že se některé předměty nepodaří detekovat, jednak snížení efektivity letecké dopravy náročnými a dlouhotrvajícími kontrolami. Jako řešení se nabízí zaměřit pozornost spíše na osoby, které nebezpečné předměty používají, než na tyto předměty samotné, a pokusit se je prověřit ještě před jejich příchodem k detekční kontrole, kterážto činnost je označována pojmem prescreening.

V další části této práce jsem nastínil jakým způsobem je prescreening prováděn ve Spojených státech amerických a Izraeli a jak je plánován ve státech Evropské unie; následně jsem popsal několik technologií, které by mohly prescreeningu posloužit. Zaměřil jsem se přitom na čtyři technologie vyvíjené v rámci systému INDECT a jejich případný přínos v prescreeningu jsem se pokusil stručně analyzovat. Jako nejpoužitelnější se jeví technologie pro zjišťování vztahů mezi osobami a organizacemi. Ukázalo se však, že u všech uvedených technologií bude zapotřebí ještě dlouhého a náročného vývoje, aby mohly být tímto způsobem implementovány.

Nakonec jsem vytvořil návrh modelu procesu prescreeningu, v němž by byly tyto technologie využity. Pro jeho případné zavedení je však nezbytný nejen důkladnější výzkum jeho jednotlivých součástí, ale také politická a diplomatická shoda a schválení potřebné legislativy.

Práci mi poněkud znesnadňovala skutečnost, že dané téma je doménou tajných služeb, které pochopitelně nemají zájem na tom, aby informace o způsobu zajišťování

bezpečnosti apod. byly dostupné laické veřejnosti, mezi niž stále patřím. Proto jsem na některých místech této práce nemohl zajít do takových podrobností a takové hloubky, jak bych si představoval. Přesto si myslím, že může být užitečná, neboť – pokud je mi známo – možnosti využití systému INDECT pro prescreening zatím nebyly nikým zkoumány. Věřím také, že bude možno na moji práci navázat a že se může stát impulsem pro další výzkum.

Velmi bych si přál, aby moderní technologie sledování lidí, jejich vztahů, soukromí, psychiky apod., kterými státy nyní disponují, nebyly nikdy zneužity totalitními režimy v neprospěch lidského pokolení ani žádného jedince.

Použitá literatura a zdroje

[1] Nařízení Evropského parlamentu a Rady (ES) č. 300/2008. In: [online]. [cit. 2014-11-28]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32008R0300&from=CS

[2] Předpis L17. In: [online]. [cit. 2014-11-28]. Dostupné z: http://lis.rlp.cz/predpisy/predpisy/dokumenty/L/L-17/index.htm

[3] BACHE, Richard, CRESTANI, Fabio, CANTER, David V., YOUNGS, Donna E. (2010) A Language Modelling approach to linking criminal styles with offender characteristics. Data & Knowledge Engineering, 69 (3). pp. 303-315. ISSN 0169-023X

[4] ELIAS, Bartholomew. Airport and aviation security: U.S. policy and strategy in the age of global terrorism. Boca Raton, FL: CRC Press, 2010. ISBN 14-200-7029-0.

[5] PRICE, Jeffrey a FORREST, Jeffrey. Practical aviation security: predicting and preventing future threats. Amsterdam: Butterworth-Heinemann/Elsevier, c2009, xxiii, 392 s. Butterworth-Heinemann homeland security series. ISBN 978-1-85617-610-1.

[6] The Aviation Security System and the 9/11 Attacks. In: [online]. [cit. 2014-11-28]. Dostupné z: http://www.9-11commission.gov/staff_statements/staff_statement_3.pdf

[7] ELIAS, Bart, William KROUSE a Ed RAPPAPORT. Homeland Security: Air Passenger Prescreening and Counterterrorism. In: [online]. [cit. 2014-11-28]. Dostupné z: http://www.au.af.mil/au/awc/awcgate/crs/rl32802.pdf

[8] AVIATION SECURITY: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks. In: [online]. [cit. 2014-11-28]. Dostupné z: http://www.gao.gov/new.items/d09292.pdf

[9] Written testimony of TSA Administrator John Pistole for a House Committee on Appropriations, Subcommittee on Homeland Security budget hearing titled "Resources for Risk-Based Security". [online]. [cit. 2014-11-28]. Dostupné z:

http://www.dhs.gov/news/2013/02/27/written-testimony-tsa-administrator-john-pistole-house-committee-appropriations

[10] BOEHMER, Jay. TSA: 40 Percent Of U.S. Travelers Now Get Expedited Screening. In: [online]. [cit. 2014-11-28]. Dostupné z: http://www.businesstravelnews.com/More-News/TSA--40-Percent-Of-U-S--Travelers-Now-Get-Expedited-Screening/?ida=Airlines&a=mgmt

[11] AVIATION SECURITY: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges. In: [online]. [cit. 2014-11-28]. Dostupné z: http://www.gao.gov/new.items/d10763.pdf

[12] MITCHELL, Chris. Israeli Security Expert: TSA Procedures 'Hysterical'. In: [online]. [cit. 2014-11-28]. Dostupné z: http://www.cbn.com/cbnnews/insideisrael/2010/November/Israeli-Security-Expert-TSA-Procedures-Hysterical/

[13] What's So Great About Israeli Security? [online]. [cit. 2014-11-28]. Dostupné z: http://www.slate.com/articles/news_and_politics/explainer/2011/01/whats_so_great_about_israeli_security.html

[14] HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS). Next Generation Screening. In: Agenda Item 8: Driving technology developments and innovation [online]. Montreal, 2012. [cit. 2014-11-28]. Dostupné z: http://www.icao.int/Meetings/avsecconf/Documents/WP%2026/HLCAS.WP.26.Next%20Generation%20Screening.FINAL%20FINAL.pdf

[15] KROUSE, William J., ELIAS, Bart. Terrorist Watchlist Checks and Air Passenger Prescreening. DIANE Publishing, 2010. In: [online]. [cit. 2014-11-28]. Dostupné z: http://books.google.cz/books?id=cpVyjXUY_Q8C

[16] SEN, Gautam. Conceptualizing security for India in the 21st Century. New Delhi: Atlantic Publishers, 2007. ISBN 81-269-0788-6.

[17] SCHNEIER, Bruce. Airport Security: Israel vs. the United States. In: [online]. [cit. 2014-11-29]. Dostupné z: https://www.schneier.com/blog/archives/2007/07/airport_securit_7.html

[18] INDECT [online]. [cit. 2014-11-29]. Dostupné z: http://www.indect-project.eu/

[19] Technology Boost for Orwell: EU to Monitor Deviant Behavior in Fight against Terrorism. In: Spiegel Online [online]. [cit. 2014-11-29]. Dostupné z: http://www.spiegel.de/international/europe/technology-boost-for-orwell-eu-to-monitor-deviant-behavior-in-fight-against-terrorism-a-656468.html

[20] Automatic Content Extraction (ACE) Evaluation [online]. [cit. 2014-11-29]. Dostupné z: http://www.itl.nist.gov/iad/mig/tests/ace/

[21] KLAPAFTIS, Ioannis. Report on current state-of-the-art of machine learning methods for behavioural profiling. INDECT Consortium, 2010.

[22] KLAPAFTIS, Ioannis. Report on current state-of-the-art methods for relationship mining. INDECT Consortium, 2009.

[23] KLAPAFTIS, Ioannis, MANANDHAR, Suresh, PANDEY, Shailesh. XML Data Corpus: Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. INDECT Consortium, 2009.

[24] Automatic content extraction 2008 evaluation plan (ace08), assessment of detection and recognition of entities and relations within and across documents. In: [online]. [cit. 2014-11-29]. Dostupné z: http://www.nist.gov/speech/tests/ace/2008/doc/ace08- evalplan.v1.2d.pdf

[25] CETNAROWICZ, Damian, DĄBROWSKI, Adam, PLEVA, Matus, JUHAR Jozef, ONDAS, Stanislav. Creation of event model in order to detect dangerous events. INDECT Consortium, 2012.

[26] File:BoardingPass SSSS.jpg. Wikimedia Commons [online]. [cit. 2014-11-29]. Dostupné z: http://commons.wikimedia.org/wiki/File:BoardingPass_SSSS.jpg

[27] Southwest (but not AirTran) joins PreCheck. TravelSkills [online]. 2013 [cit. 2014-11-29]. Dostupné z: http://travelskills.com/2013/11/15/southwest-airtran-joins-precheck/