

PŘEDBĚŽNÉ HODNOCENÍ CESTUJÍCÍCH ZA ÚČELEM ZVÝŠENÍ BEZPEČNOSTI CIVILNÍHO LETECTVÍ

PRELIMINARY PASSENGERS ASSESSMENT TO INCREASE SECURITY IN CIVIL AVIATION

Daniel MARŠÁLEK, Ondrej PALATÁŠ, Radomír ŠČUREK
daniel.marsalek@prg.aero, ondrej.palatas@centrum.sk, radomir.scurek@vsb.cz

Došlo 2. 9. 2012, přijato 25. 1. 2013.

Dostupné na http://www.population-protection.eu/attachments/044_vol4n4_marsalek_palatas_scurek.pdf.

Abstract

Preliminary passengers assessment as one of the essential parts in ensuring the security of civil aviation - this is a subject of the submitted article. In the beginning of the paper, it describes current status, including several of its modifications. In the second part of the text, system is optimized, both in terms of protection of passenger data, and in terms of increased security. The system is able to compare, in the real-time, data from multiple databases and based on this establish the status of the passenger. All this even before arriving at the airport for departure.

Key words

Airport, attack, CAPPS, database, optimalization, passenger, security, preliminary assesment, terrorism.

Letecká doprava, v současné době, přináší cestujícím nízkou míru anonymity. Mohou za to především opakované kontroly totožnosti cestujících. Cestující poskytuje dopravci své jméno a příjmení, existují záznamy o objednavce a zaplacení letenky. Při vstupu do tranzitního prostoru a následně do letadla jsou cestujícím kontrolovány cestovní doklady, některé státy vyžadují po cestujících údaje o národnosti, bydlišti, místě pobytu v cizí zemi, dokonce i o profesi a všechny tyto údaje jsou uschovány v databázi. Rozeznáváme údaje PNR (Passenger Name Record), což je digitální záznam o cestujícím, o jeho cestě konkrétní leteckou společností. Databáze PNR jsou určeny pro letecké společnosti, které jsou spravovány centrálně v databázi GDS (Global Distribution Systems). Mezi nejrozšířenější globální distribuční systémy patří v USA užívaný systém SABRE a GALILEO/APOLLO. V Evropě se využívá systém AMADEUS, který používá např. ČSA. Záznam ve shora uvedené databázi je proveden vždy současně s rezervací letenky. Jakmile systém záznam vytvoří, vygeneruje současně auditní protokol, do kterého se zaznamenávají veškeré změny záznamu. Také se zde postupně ukládají údaje o čase, místě rezervace, uživatelském identifikačním čísle,

údaje o zprostředkovateli, cestovní kanceláři a konkrétní osobě, která provedla do systému záznam, stejně jako jméno cestujícího, nebo subjektu, který později provedl změnu rezervace. Data jsou předána ve společně mezinárodní dohodnuté formě, resp. formátu, který se nazývá AIRIMP. V případě pravidelného zákazníka letecké společnosti je vytvořen profil, kde se přidávají jednotlivá data o následující cestě (např. čísla kreditních karet, čísla pasů, elektronické adresy, telefonní čísla, adresa, informace o rodinných příslušnících, poznámky o preferovaném jídle a sedadle v letadle, zdravotním stavu, poznámky z cestovní kanceláře aj.). Většina dat zadaných do digitálního záznamu o osobě cestujícího nejsou vkládány leteckými společnostmi, ale cestovními kanceláři nebo samotným cestujícím za účelem zvýšení komfortu cestování [7].

V současnosti se zvýšenými bezpečnostními riziky v letecké dopravě rozeznáváme rovněž tzv. další informace o cestujícím, označené API (Advance Passenger Information). Tyto údaje jsou požadovány imigračními úřady některých států. Pokud letecká společnost tyto údaje o cestujícím neposkytne, hrozí jí pokuty, nebo i zákaz vstupu do vzdušného prostoru dané země. Mezi tyto údaje patří zpravidla data obsažená v cestovních dokladech, navíc pak údaje o trvalém bydlišti, délce plánovaného pobytu, nebo telefonní kontakty. Na rozdíl od PNR neslouží API žádným obchodním účelům.

Letecké společnosti mají dvě možnosti jak poskytovat požadovaná data bezpečnostním složkám států, do kterých létají. Jedná se o způsoby PUSH a PULL nebo jejich kombinace. Nejpoužívanější je systém PUSH, který spočívá v tom, že letecká společnost shromáždí veškerá data o cestujících a daném letu ve svých databázích a zpravidla ještě před odletem je odešle bezpečnostním složkám daného cílového státu. V systému PULL jsou informace shromážděny v databázích letecké společnosti a bezpečnostní orgány cílové země mají přístupová hesla a sami si potřebné údaje v databázi letecké společnosti kdykoliv vyhledají.

Za účelem boje proti nedovolenému přistěhovalectví a zdokonalení hraniční kontroly byla vydána směrnice Rady EU č. 82/2004, která ukládá leteckým dopravcům povinnost o každém cestujícím poskytnout devět základních údajů [6]. Jedná se o:

- jméno a příjmení,
- datum narození,
- číslo a typ použitého cestovního dokladu,
- státní příslušnost,
- údaj o hraničním přechodu na území členského státu EU,
- kódové číslo letu,
- čas odletu a příletu,
- celkový počet osob přepravovaný daným letem,
- počáteční místo nástupu na palubu letadla.

V České republice byla tato povinnost zavedena od 1. 7. 2006 v rámci novely zákona č. 49/1997 Sb., o civilním letectví ve znění změn a doplnění. Vzhledem k náročnosti na zpracování vyžaduje Policie České republiky tyto údaje pouze od dopravců létajících z rizikových destinací, tedy ze zemí s největším

počtem ilegálních emigrantů [7]. Údaje o cestujících nejsou využívány jen pro operativní bezpečnostní složky daného státu, ale také k identifikaci obětí leteckých nehod.

V USA jsou data cestujících směřujících do jejich země podrobena navíc další dvojstupňovou kontrolou. V prvním stupni jsou letecké společnosti povinny prověřit, zda některý z cestujících nebo posádky není zařazen na seznamech nežádoucích osob. Tyto seznamy jsou označeny NO FLY nebo SELECTEE list. Jde o seznamy osob podezřelých z terorismu, které jsou poskytnuty bezpečnostními složkami USA leteckým společnostem včetně aktualizací. Pokud letecká společnost nalezne na seznamech takového cestujícího, je povinna prostřednictvím zastupitelského úřadu informovat bezpečnostní úřady USA. Takoví cestující nejsou na palubu letadla vpuštěni, nebo na základě instrukcí bezpečnostních složek bez upozornění dopraveni na území USA a zde jsou podrobeni zvláštním opatřením. Druhý stupeň prověření cestujících do USA je prováděn těsně před odletem letadla. Musí být již odeslána, nebo zpřístupněna API data do Národního sledovacího centra USA (National Tracking Centre), které opět prověřuje seznamy cestujících a porovnává je se seznamy NO FLY nebo SELECTEE. Pokud jsou takoví cestující i přes kontrolu leteckých společností zjištěni, je upozorněno Středisko pro informace o teroristech USA (Terrorist Screening Centre), které vydá doporučení, zda osoba nebude vůbec vpuštěna, nebo po přeletu zatčena, či jen sledována. Podle toho v jaké fázi se letadlo nachází, může být let odkloněn, nebo nařizeno vrátit se do výchozí destinace. Údaje API jsou vyžadovány, pokud letadlo jen nad územím USA přelétá [6].

Zavedení systému předběžného hodnocení cestujících

Vzhledem k rostoucím nárokům na bezpečnost letišť se klade důraz na vývoj a zavádění integrovaného bezpečnostního systému, který je napojen na odbavovací, bezpečnostní a vyhledávací systémy (SITA). Prvním systémem hodnocení cestujících v letecké dopravě z hlediska možných rizik násilných činů, byl systém CAPPs (Computer Assisted Passenger Pre-screening System – počítačový systém předběžného hodnocení cestujících), vytvořený ve druhé polovině 90. let minulého století v USA. Organizace TSA (Transportation Security Administration) vede na základě amerického předpisu 49 USC § 114 odst. h) odst. 2), seznam osob, které jsou podezřelé z terorismu nebo leteckého pirátství a jsou hrozbou pro letecké společnosti a státní bezpečnost [1]. Systém CAPPs pracoval s uvedeným seznamem a byl založen na předběžné identifikaci teroristů, kteří se pokoušejí koupit letenky na paluby letadel v USA. Tento systém byl založen na analyzování údajů o cestě, které běžně shromažďují letecké společnosti. Systém CAPPs byl provozován FBI (Federální úřad pro vyšetřování USA) a FAA (Federální úřad pro letectví USA) a do plného provozu byl spuštěn v roce 1997. Pokud byl některý z cestujících vybrán jako potencionální bezpečnostní hrozba, byla jeho zavazadla podrobena důkladnější kontrole. Cestující sám žádnou podrobnější prohlídkou neprocházel. To se ukázalo být slabinou systému CAPPs,

protože ten 11. září 2001 správně identifikoval většinu atentátníků jako potencionální hrozbu, ale protože jejich zavazadla prošla kontrolou bez problémů, byli všichni vpuštěni na palubu letadel. Po útocích z 11. září 2001 bylo zřejmé, že dosavadní bezpečnostní systémy v letecké dopravě jsou snadno překonatelné. Proto byl roku 2003 předložen TSA systém CAPPS II, který byl navržen organizací ONRA (Office of National Risk Assessment – Úřad pro národní hodnocení rizik). TSA měla oproti předchozí verzi systému následující požadavky:

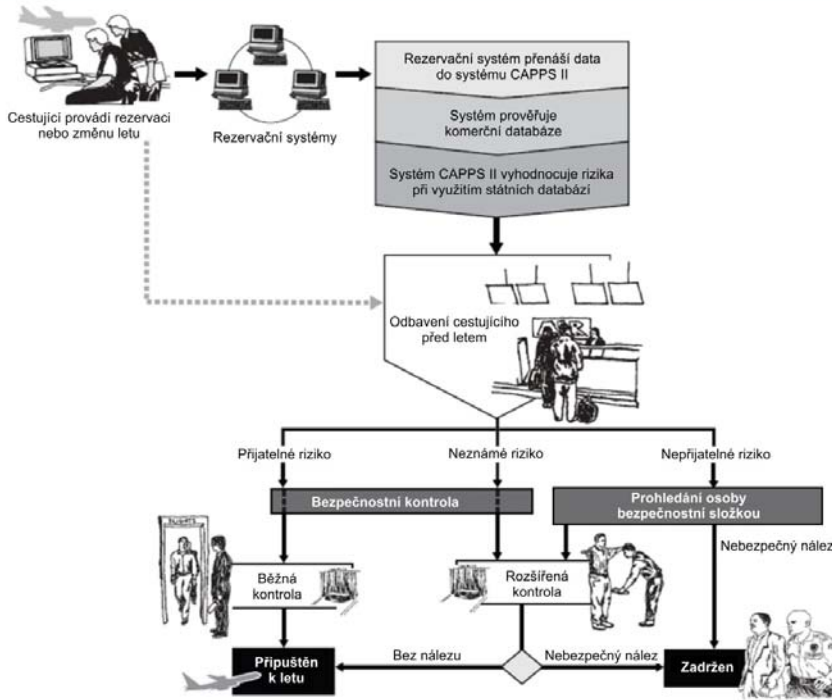
- Systém bude plně spravován vládou, nikoli leteckými společnostmi
- Kontrole budou podrobeni všichni cestující vyhodnocení systémem jako potenciální hrozba, bez ohledu na bezpečnostní kontrolu jejich zavazadel
- Systém se musí vztahovat na každou leteckou společnost a každé letiště

Oproti předchůdci byl systém CAPPS II postaven na analyzování dat na základě křížových dotazů. Data z PNR byla porovnávána s dalšími údaji uloženými ve státních a komerčních databázích. Navíc by se ověřovala totožnost, zjišťovaly se předchozí kriminální aktivity, ale také to, zda daný cestující nemá možné vazby na teroristy. Systém provede, na základě vstupních dat, výpočet "skóre rizika" a to uvede pomocí barevné škály na palubní vstupenku s uvedením odpovídající úrovně následné bezpečnostní kontroly pro danou osobu: zelená (bez ohrožení) představuje žádnou další bezpečnostní kontrolu, žlutá (neznámé nebo možné ohrožení) znamená další screening, a červená barva (vysoké riziko) neumožní držitelé palubní vstupenky nastoupit na palubu letadla a bude zadržen a předán příslušným orgánům. Níže je uvedeno schéma jeho fungování, nicméně přesný algoritmus výpočtu skóre nebyl nikdy zveřejněn a podléhá obchodnímu tajemství TSA.

Návrh na zavedení systému CAPPS II naráží na problém s procházením řady databází, obsahujících soukromé údaje, čímž vzbuzuje protesty ochránců lidských práv. Zavedení tohoto systému bylo proto v srpnu 2004 pozastaveno. V americké společnosti podobné pokusy nevzbuzují zrovna nadšení. Řada občanů USA vnímá nasazení podobných systémů do praxe jako automatickou ztrátu své ústavně chráněné svobody a narušení základních práv a svobod. Především organizace EFF (Electronic Frontier Foundation) silně oponuje proti zavádění systému CAPPS II a snaží se bojovat proti jeho realizaci. Kromě podání formálních připomínek k CAPPS II na ministerstvo vnitřní bezpečnosti, vede EFF výzvu za soukromé cestování bez sledování ze strany státních úřadů [3]. Např. občanští liberálové v americkém parlamentu argumentují, že v rámci programu neexistují stále dostatečné mechanismy odškodnění nevinných občanů, kteří se mohli (např. chybou systému) objevit na seznamu sledovaných osob.

Na začátku roku 2005 byl CAPPS II nahrazen novým programem (Secure Flight), který vychází ze systému CAPPS II. Vzhledem k pokračujícím obavám z narušování soukromí však byl i tento program zablokován americkým kongresem do doby, než vláda prokáže, že systém projde testy na přesnost na ochranu soukromí. TSA si v rámci implementace tohoto programu kladlo za cíl prověřit 100 % všech tuzemských (amerických) komerčních letů do počátku roku 2010 a

100 % všech mezinárodních komerčních letů do konce roku 2010. Tento program není stále plně funkční a jeho postupné zavádění stále probíhá. [2].



Obr. 1

Schéma fungování systému CAPPS II. Vlastní tvorba, vycházeno z internetového zdroje [6]



Obr. 2

Schéma fungování systému Secure Flight. Vlastní tvorba, vycházeno z internetového zdroje [5]

Je tento systém výměny údajů dostačující pro bezpečnostní účely?

Při bližším pohledu na dnešní situaci v oblasti poskytování API údajů jednotlivým bezpečnostním složkám konkrétních států můžeme pozorovat zjevnou diskontinuitu. Ta vyplývá z neharmonizované správy a poskytování API údajů. Další odlišnost je v přiřkládání vážnosti API údajům v jednotlivých regionech. Tyto údaje hrají klíčovou roli v bezpečnostní politice TSA, která se týká vpouštění cizích státních příslušníků na území USA. Ale je to skutečně efektivní? S určitostí můžeme říci, že ne na 100 %. Vypovídají o tom případy pokusů o ohrožení letů směřujících do USA. Asi nejznámějším je tzv. "Vánoční bombový pokus", který se odehrál dne 25. 12. 2009 na lince společnosti Northwest Airlines z Amsterdamu do Detroitu. Pachatel, kterým byl Nigerijec Umar Farouk Abdulmutallab, se bez menších problémů dostal na palubu letadla i s NVS ukrytou ve spodním prádle s úmyslem odpálit ji nad územím USA. A to i přesto, že se nacházel na seznamu NO FLY jako osoba podezřelá ze spolupráce s teroristy. Tento případ ale ukazuje další velmi závažnou mezeru v americkém systému práce s API údaji. Konkrétně jde o prověřování osob letících do USA porovnáváním se seznamy NO FLY a SELECTEE. Problém je v tom, že první kontrolu dělají samotné letecké společnosti a tak TSA ani NTC nemají žádný vliv na ověření správnosti výsledků této prvoinstanční kontroly. Druhá kontrola je již prováděna pod taktovkou NTC. Nicméně tato kontrola probíhá těsně před odletem, častěji se však stává, že až během letu. Primárním úkolem NTC a TSA a jejich NO FLY a SELECTEE seznamů je zamezit vstupu osob spolupracujících s teroristickými organizacemi na území USA. Jaksi se ale zapomíná, že teroristický útok je možné spáchat i během přeletu nad územím USA nebo při přiblížení na letiště nad velkou metropolí. Může být mířený proti letadlu patřícímu letecké společnosti z USA nebo také proti americkým občanům na palubách zahraničních leteckých společností létajících do USA. Tyto scénáře by měly vylučovat vysoké bezpečnostní standardy zavedené v jednotlivých zemích a společenstvích, ale jak nám ukazuje praxe, někdy tomu tak nebývá.

Dalším neméně důležitým faktorem je sestavování a aktualizace seznamů NO FLY a SELECTEE a druhy údajů, které identifikují osobu na seznamech. Nezřídka se setkáváme s případy, že na palubu letadla není vpuštěna osoba (dítě, důchodce), která je omylem považována za osobu spolupracující s teroristy, i když se evidentně jedná o omyl (zejména v případě malých dětí). Proto by bylo vhodné sladit API údaje s údaji, které figurují na seznamech NO FLY a SELECTEE tak, aby nedocházelo k záměně osob.

V tomto okamžiku můžeme vyslovit myšlenku, že API údaje představují pro USA spíše nástroj prevence vstupu nežádoucích osob na území USA, než nástroj ochrany civilního letectví. Pokud tvrdíme, že pro USA tyto specifické údaje představují nástroj prevence, tak v Evropské unii jde jen o jakýsi módní doplněk. Je to podmíněno zejména tím, že v současné době je velká část států zapojena do Schengenského prostoru, kde je garantován svobodný pohyb osob a zboží. S určitým nadnesením můžeme říci, že i kvůli této skutečnosti jsou letecké

společnosti a bezpečnostní složky legislativou nuceny "ignorovat", koho vpuštějí na palubu.

Taková generalizace evropského prostoru ale není úplně na místě. Samozřejmě i v Evropě, či přímo v EU působí státy, které nejsou začleněny do Schengenského prostoru a dokonce uplatňují vůči jiným zemím vízovou povinnost. V takovém případě hrají API údaje důležitou roli. Také by měly sloužit jako nástroj pro potlačení nelegální migrace obyvatelstva. Ale jak dokazují statistiky nelegální migrace, i v tomto směru lze využívání API údajů posunout na vyšší úroveň.

(Ne)fungování systémů předběžného hodnocení cestujících

Postupem času přicházejí odpovědné orgány na to, že chovat se ke každému cestujícímu jako k hrozbě je kontraproduktivní. Prvním problémem takové politiky je nadměrné zatěžování bezpečnostních složek zabezpečujících detekční kontrolu cestujících. Snižuje se poměr – penetrace osob za jednotku času. Pracovníci detekční kontroly jsou vystavováni nadměrné zátěži, a tím jsou náchylnější k fatální chybě. Často dochází ke zpoždění letů, což způsobuje problémy leteckým společnostem a provozovatelům letišť a letových navigačních služeb.

Druhým problémem je nepřímé „odrazování“ cestujících od využívání letecké dopravy zaváděním přísných opatření, které často zacházejí až za hranice přípustnosti. Znechucení cestujících pak bojkotují leteckou dopravu a hledají jiné způsoby přepravy. To ekonomicky poškozuje jak letecké společnosti, tak i provozovatele letišť (a v rámci nich i bezpečnostní složky, přímo odpovědné za uplatňování bezpečnostních pravidel).

Rapidní rozvoj letecké dopravy, který se očekává po odeznění krize, s sebou přinese nárůst cestujících, a tím i potřebu urychlit procesy související s ochranou letectví při kontinuálním zvyšování bezpečnostních standardů. Aby bylo možné tento požadavek splnit, bude muset projít bezpečnostní politika ochrany civilního letectví určitými změnami. Jednou ze změn bude zařazení sběru specifických osobních údajů o cestujícím do systému detekční kontroly, která se následně rozdělí na několik stupňů, kde první stupeň kontroly proběhne ještě před příchodem cestujícího na letiště. Na této myšlence je založen i níže představený a navržený systém.

První pokusy s takovými systémy v USA ukazují, že je velmi důležité brát velký ohled na to, s jakými údaji takový systém pracuje. Při navrhování je nutné zvážit, jaké databáze, a v rámci nich informace, budeme využívat v prověřovacím procesu. Americké organizace na ochranu základních práv a svobod ostře vystupují proti jakýmkoli pokusům využívat osobní informace shromážděné ve státních a komerčních databázích při ochraně civilního letectví. V budoucnu se takovému kroku ale nevyhneme. Přesto při tvorbě následujících systémů musíme mít vždy na zřeteli primární cíl, a tím je co nejvyšší možná ochrana osobních údajů a nedotknutelnost a svrchovanost osoby jako takové.

Jak vyplývá z popisů fungování stávajících systémů na předběžné hodnocení cestujících, ty obsahují řadu problémů především s vyhodnocováním a

zpracováním identifikovaných rizik a nastavením následných postupů ze strany státních a bezpečnostních složek. Současné systémy nereflktují aktuální hrozby a principy tzv. asymetrických ohrožení.

Níže navržený systém tyto nedostatky řeší a objektivně posuzuje možná rizika ohrožení civilního letectví. A co je důležité, celý systém je navržen tak, aby byla rizikovost konkrétní osoby (hodnota score) identifikována ještě před jeho nástupem na palubu letadla, a co víc, ještě dřív, než se cestující dostaví na letiště k odletu a přistoupí k bezpečnostní kontrole.

Návrh systému profilace a kategorizace pasažérů před detekční kontrolou

Návrh systému je v tomto příspěvku omezen na popis schématu a algoritmu jeho fungování, který se rozpadá na 4 na sebe navazující segmenty. Proces začíná u rezervačních rozhraní dopravců (rezervace letenek přes internet, prostřednictvím cestovní agentury, agenta letecké společnosti, call centrum, externích prodejců letenek apod.) a končí přidělením konkrétního statusu prověřované osoby. Z důvodu bezproblémové implementace systému do praktického provozu reflektuje použití stávajících provozních rozhraní leteckých společností. V závislosti na tom lze při jeho případném zavádění ušetřit značné finanční prostředky a snížit také časovou náročnost této operace.

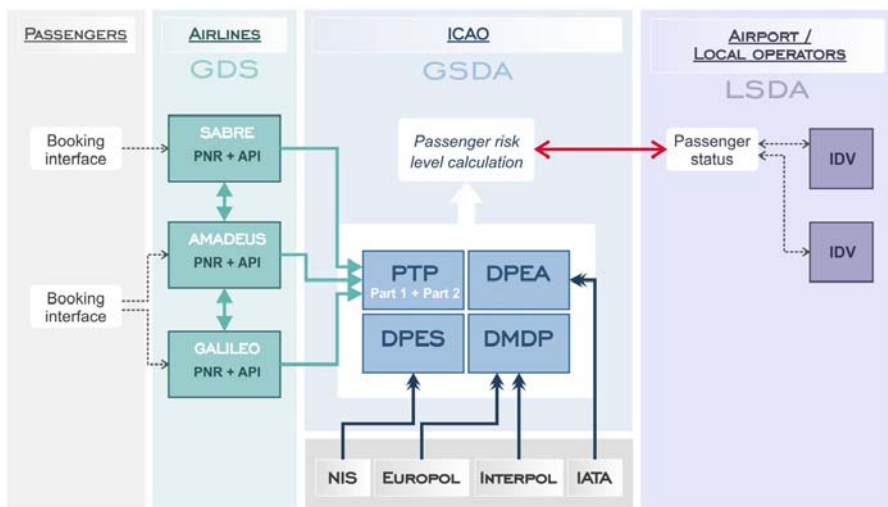
Prvním segmentem navrhovaného systému je klasické rezervační rozhraní konkrétního dopravce, odkud jsou informace o cestujícím (PNR a API) pomocí datového toku posílány do GDS (globální distribuční systém), kde se uchovávají. Odtud jsou pak buď metodou PUSH, PULL, nebo jejich kombinací přenášena k bezpečnostním složkám v cílové destinaci. Následuje zařazení stěžejního segmentu, tzv. GSDA (Global Security Database for Aviation). Jedná se o externí, nadnárodní expertní systém posuzující rizikovost jednotlivých cestujících a je nezávislý na databázích leteckých společností.

GSDA dále obsahuje následující databáze:

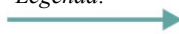


- PTP (Passenger Travel Profile) – Jedná se o profil cestujícího, který bude obsahovat informace o jeho letech, destinacích, příslušnosti k věrnostnímu programu dopravce, jeho aktuálních rezervacích, vízech, cestovatelských návycích (třída ve které nejraději cestuje, zda využívá zapsaná zavazadla, zda se někdy nedostavil k odletu apod.).
- DPES (Database of Potentially Endangered Subjects) – Databáze potenciálně ohrožených subjektů, jako letiště, aerolinie a osoby. Půjde o samostatnou databázi obsahující bezpečnostně relevantní informace o možných hrozbách.
- DPEA (Database of People Excluded from Aviation) – Databáze osob vyloučených z letecké dopravy představuje obdobu amerického seznamu osob, které jsou vykázány z letecké přepravy z důvodu spolupráce s teroristickými a extremistickými organizacemi, trestně stíhané osoby, osoby, které se dopustily násilí na palubě letadla, resp. v objektu spadajícím pod specifický paragraf trestního zákona apod.

- **DMDP (Database of Missing and Dangerous People)** – Databáze pohřešovaných a nebezpečných osob, která bude aktualizována organizacemi INTERPOL a EUROPOL, tak aby byla včas identifikována osoba na útěku, osoba která byla unesena nebo je monitorována policií pro nezákonnou činnost.

Algoritmus fungování navrženého systému je uveden na obr. 3. Kromě datového toku ze strany leteckých dopravců (zelená barva) budou do systému GSDA vstupovat údaje národních a nadnárodních bezpečnostních a zpravodajských služeb, jako EUROPOL, INTERPOL (modrá barva). Pro zajištění výstupu na konkrétním letišti bude na GSDA přímo navázán (červená barva) modul LSDA (Local Security Database for Aviation). Z pohledu architektury systému může být koncový modul LSDA umístěn buď v daném státě a bude společný pro více letišť, nebo jej lze umístit na konkrétním letišti a pak bude sloužit výhradě jemu. Finálnímu rozhodnutí o umístění modulu LSDA musí předcházet provedení hloubkové analýzy, která musí posuzovat výhody/nevýhody daného způsobu umístění, klást důraz na bezpečnostní prvky databáze a datových toků a v neposlední řadě přihlížet k finanční náročnosti daného řešení. Na modul LSDA budou pak přímo napojené koncové zařízení (IDV – Identity vericator) sloužící k individuální identifikaci cestujících a přiřazení bezpečnostního statusu.



Legenda:

-  PNR a API informace ve formátu AIRIMP
-  Informace od mezinárodních bezpečnostních subjektů
-  Komunikační kanál mezi Global a Local Security Database for Aviation (GSDA – LSDA)
- NIS – National Intelligence Services (Národní zpravodajské služby)
- IDV – Identity vericator

Obr. 3

Algoritmus fungování navrhovaného systému pro předběžné hodnocení cestujících.
Vlastní tvorba

Z pohledu datového toku lze celý proces popsat následovně:

1. fáze:

Po zadání příslušných informací do rezervačního systému cestujícím, resp. osobou provádějící rezervaci, se vytvoří standardní záznam formátu AIRIMP do GDS. Odtud budou informace o rezervaci a cestujícím automaticky posílány do modulu GSDA.

2. fáze:

V GSDA se na základě získaných informací vytvoří PTP. PTP bude sestávat ze dvou nezávislých a navzájem propojených modulů. První modul (Part 1) bude obsahovat pouze identifikační údaje osoby a automaticky vygenerovaný specifický identifikátor (primary key). Druhý modul (Part 2) bude obsahovat samotný profil pasažéra a výše zmiňovaný identifikátor, který bude vytvářet relaci dat X [Part 1; Part 2] a bude přesně identifikovat konkrétní osobu. Oddělením PTP od osobních údajů zajistíme vyšší stupeň jejich ochrany.

3. fáze:

Modul GSDA shromažďuje 4 báze dat, do kterých bude zajišťovat přísun aktuálních relevantních informací do jednotlivých segmentů. GSDA na základě všech dostupných informací vytvoří den před odletem cestujícího jeho "status". Informace o všech cestujících, kteří mají následující den plánovaný let z daného letiště, systém exportuje do šifrovaného packetu a automaticky zašle na konkrétní LSDA.

Poznámka: Komunikace mezi GSDA a LSDA bude kromě posílání packetu v pravidelných intervalech spočívat i v zaslání aktualizovaných informací v případě, že dojde ke změně nějakého elementu (např. akutní výskyt nebezpečí v určité destinaci).

4. fáze:

Cestující se před vstupem na stanoviště bezpečnostní kontroly identifikuje pomocí biometrického dokladu a LSDA mu přiřadí jeho status. Poté cestující přistoupí k bezpečnostní kontrole. Po provedeném letu cestujícího a potvrzení z GDS se v PTP vytvoří záznam, že pasažér daný let absolvoval.

Co se změní po zavedení takového systému?

Implementací navrhovaného systému získáme možnost provést první stupeň předběžného hodnocení osoby ještě před tím, než fyzicky dorazí na letiště, a díky reportu ze systému GSDA lze s dostatečným předstihem identifikovat ty osoby, které představují potenciální hrozbu. Na základě toho budeme moci přistoupit k zavedení systému rozpoznávajícího tzv. známé a neznámé cestující a spolu s přiděleným statutem je podrobovat různým stupňům bezpečnostní kontroly podle míry rizika, kterou představují. Na základě aktualizovaných údajů z GSDA bude systém schopen odhalit osobu na útěku, unesenou osobu nebo monitorovat

pohyb zájmové osoby. Po zavedení seznamů NO FLY a SELECTEE v rámci evropského prostoru bude možné zamezit vstupu na palubu letadla takové osobě, která se bude nacházet v uvedených seznamech (osoba v režimu STOP FLY). Díky propracovanému a zautomatizovanému systému algoritmicizace nebude možné monitorovat nezájmovou osobu. Pokročilejší způsob zpracování osobních údajů osob zajistí vysokou míru jejich ochrany a současně využívání pouze nejnútnejších údajů pro zajištění bezpečnosti a ochrany civilního letectví. Inovace navrženého systému spočívá v několika bodech.

- Striktně oddělený segment systému pro letecké dopravce se segmentem spravovaným mezinárodními organizacemi.
- Efektivnější práce se vstupními daty – data uložená v jednotlivých databázích (modulech) mají přesně nadefinované správce a přístupová místa. Jejich zabezpečení se řídí předpisy platnými pro správu databází s osobními údaji a citlivými informacemi.
- Oddělení údajů o cestujícím v jeho profilu – ke spárování dat dochází až těsně před samotným výpočtem hodnoty score na základě propojení dvou shodných identifikátorů. Díky diverzifikaci osobních údajů nedochází k přímému ztotožnění osoby a možnému zneužití osobních dat.
- Kalkulace výsledného score den před daným letem. V případě identifikace stíhaných, pohřešovaných nebo nežádoucích osob (např. teroristů) lze alarmovat bezpečnostní složky letiště dřív, než se daná osoba dostaví na letiště.
- Jednotný správce modulu GSDA – správu bude zajišťovat organizace ICAO – bezpečnostní sekce. Tím lze předcházet případným nefunkčností jednotlivých databází a vyššími nároky na budování infrastruktury.
- Příprava na budoucí implementaci sdílených security checkpointů pracující na základě přiděleného statusu cestujícího (např. Checkpoint of the Future od IATA). Tyto screeningové systémy jsou totiž schopny přizpůsobovat hloubku prováděné bezpečnostní kontroly na základě předem vytvořeného statusu určujícího míru rizika konkrétního cestujícího, a to automaticky, bez jakéhokoliv zásahu ze strany obsluhy.
- Příprava na zavedení systému iBorders, který umožňuje identifikaci cestujících pomocí strojově čitelných kódů a biometrických parametrů v cestovních dokladech, zejména pomocí otisků prstů, geometrie tváře a otisku duhovky.

Myšlenka existuje ale co dál?

Samotnému vytvoření takového systému musí předcházet nutná legislativní úprava stávajících zákonů; široká diskuse odborné veřejnosti, ale hlavně ochota spolupráce státních orgánů, zainteresovaných bezpečnostních orgánů, institucí zastřešujících civilní letectví, provozovatelů letišť a leteckých společností. Nemalou roli v tomto procesu bude hrát i vůle spolupracovat

s cestující veřejnosti a ostatními subjekty participujícími na ochraně práv a svobod cestujících a osob jako takových, protože úspěšnost takového projektu bude záviset na reakci veřejnosti.

Literatura

- [1] CORNELL UNIVERSITY LAW SCHOOL. LEGAL INFORMATION INSTITUTE. 49 USC § 114 – Transportation Security Administration [online]. [cit. 2012-08-20]. Dostupné z: http://www.law.cornell.edu/uscode/text/49/114#h_2
- [2] MERARI, A. Terrorism as a Strategy of Insurgency. *Terrorism and Political Violence*. 2001, vol. 5., 4, s. 213–251.
- [3] ELETRONIC FRONTIER FOUNDATION. CAPPS II: Government Surveillance via Passenger Profiling [online]. [cit. 2012-08-15]. Dostupné z: <http://w2.eff.org/privacy/cappsii/>
- [4] ACLU – AMERICAN CIVIL LIBERTIES UNION. Secure Flight Re-Engineering Welcomed but Watchlist Problems Remain Unaddressed [online]. [cit. 2012-08-15]. Dostupné z: <http://www.aclu.org/technology-and-liberty/secure-flight-re-engineering-welcomed-watchlist-problems-remain-unaddressed>
- [5] TRANSPORTATION SECURITY ADMINISTRATION. Secure Flight Program [online]. [cit. 2012-08-18]. Dostupné z: http://www.tsa.gov/what_we_do/layers/secureflight/
- [6] GAO. Report to Congressional Committees. Aviation Security – Computer-Assisted Prescreening System Faces Significant Implementation Challenges [online]. [cit. 2012-08-15]. Dostupné z: <http://www.gao.gov/new.items/d04385.pdf>
- [7] KOVERDYNSKÝ, Bohdan. *Bezpečnost civilního letectví: historie, organizace, standardy, postupy*. Praha: Odbor bezpečnostní politiky MV ČR, 2007. 104 s.
- [8] ŠCUREK, Radomír, Pavel ŠVEC. *Ochrana letiště před protiprávními činy*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2009. 135 s. ISBN 978-80-7385-071-5.