Bezpečnostní mechanismy značkování dat

Data-tagging Security Mechanism

Ing. Jan Ryšavý

Bakalářská práce 2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ing. Jan Ryšavý**
Osobní číslo:	**A13806**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnostní mechanismy značkování dat**
Téma anglicky:	**Data-tagging Security Mechanisms**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma bezpečnostních mechanisů značkování dat.**
2. **Popište způsoby propojení informačních systémů s různými stupni utajení.**
3. **Navrhněte softwarový způsob crossdomain řešení značkování dat .**
4. **Aplikujte vlastní návrh řešení na fiktivní informační systém a jeho propojení se systémy s různým stupněm utajení.**
5. **Vyhodnoťte zvolený způsob bezpečnostního mechanismu značkování dat.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Gope, Dejan. Cluster Based Data Labeling for Categorical Data: Data Labeling For Categorical Data Into Clusters Based On The Important Attribute Values. LAP LAMBERT Academic Publishing, 2013. 116 s. ISBN 978-3659321405.**
2. **S. Department of Defense. Information Assurance (IA) Policy for Space Systems Used by the Department of Defense [online]. Dostupné z WWW http://www.dtic.mil/whs/directives/corres/pdf/858101p.pdf**
3. **Knopová Martina. Bezpečnost dat v informačních systémech [online]. Dostupné z WWW http://ikaros.cz/bezpecnost-dat-v-informacnich-systemech**
4. **Miroslav Ludvík; Bohumír Štědroň. Teorie bezpečnosti počítačových sítí. Computer Media. 2008. 98 s. ISBN 978-80-8668-635-6.**
5. **Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.**

Vedoucí bakalářské práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **26. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Praze, dne …….

podpis diplomanta

ABSTRAKT

Předložená bakalářská práce s názvem „Bezpečnostní mechanismy značkování dat“, se věnuje možnostem zabezpečení informací v elektronické podobě. V první části je popsán důvod, účel a cíl použití tohoto typu zabezpečení, legislativní východiska a technické parametry. Druhá část je věnována implementaci možné realizace bezpečnostního mechanismu značkování do stávající fiktivního informačního systému. Cílem práce je pojednat o možnostech tohoto typu zabezpečení dat a informací a podat základní možný způsob jeho implementace.

Klíčová slova: IEG, bezpečnostní značkování, bezpečnostní prověření, bezpečnostní politika, XML SPIF

ABSTRACT

The submited bachelor thesis, titled: "Data-tagging Security Mechanism“ analyses using and possibilities of security labelling and labels. In first part we can find purpose of using Security labelling mechanism, its general and specific technical description and appropriate national legislative. Second part focus is on implementation of Data Labelling Mechanism into existing fictional information system. Objective of this thesis is to famillliarize reader with Security Labelling topic a suggest way ahead for implementation such a mechanism into existing information system.

Keywords: IEG, Datalabelling, Security Labelling, Security Label, Security Clearance, Security Policy, XML SPIF

Velmi děkuji své rodině za podporu, kterou mi věnovala po celou dobu studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

1 ÚVOD

Propojením dvou (a více) informačních systémů se rozumí spojení (propojení) informačních systémů za účelem jednocestného nebo obousměrného sdílení informací.

V tomto dokumentu bude popisováno propojení dvou informačních systémů různého stupně utajení. V práci budou použity znalosti, termíny, normy a odkazy z vojenského prostředí. Stejně jako vojenské i další informační systémy mají svá specifika a je nezbytné dodržet určitá pravidla pro zabezpečení jejich propojení se systémy jiného (většinou nižšího) stupně utajení, např. systémy civilními.

Převedeme tuto teorii do reálné praxe. Nezbytným prvek pro dosažení úspěchu v dnešních civilně-vojenských operacích na udržení míru, reakce na živelnou pohromu a operace spolupráce civilního a vojenského sektoru je zabezpečení komunikace a rychlá a efektivní výměna dat a informací. Jedná se např. o preventivní a rekonstrukční týmy, výstavbu škol za spolupráce armády a jiných zařízení občanské vybavenosti a další pomoc občanům žijících v oblastech postižených válečným konfliktem.

Civilní organizace (NGO – Non Govermental Organization, dle definice NATO), jako např. Červený Kříž, jsou nezávislé entity, které sami spravují velkou škálu různých programů. K této práci potřebují a požadují mnoho informací a zajištěných informačních toků, jako jsou:

- meteorologická situace a geografické podmínky,
- politický, sociální a ekonomický vývoj v regionu,
- ceny trhu za různé komodity, za dopravu a doručení,
- spolupráci s OSN a potažmo s vojenským sektorem,
- aktivitu populace, demografický vývoj, pohyby populace a vývojové křivky,
- mezinárodní logistická spolupráce a plánování.

Civilní organizace během konfliktu, nebo krize, sbírají data z mnoha zdrojů, od jiných civilních organizací, dárců (existují i dárci informací, kteří svými dary podporují chod nezávislé, nebo neziskové organizace), vojenské zprávy, zprávy zpravodajských agentur, zprávy tiskových agentur, úřední desky různých lokálních a mezinárodních úřadů a také sběr informací od samotných obětí konfliktu.

Civilní organizace nemají schopnosti získávat všechna podobná data vlastní cestou, tak jak by bylo potřebné a sdružují se do větších celků, které mají vyjednánu informační podporu. Informační podpora je poskytována ze strany vojenských složek nebo zpravodajských služeb.

Pokud je civilní organizace na území válečného konfliktu, musí být schopná sdílet a vyměňovat data s dalšími komunitami, státy, vládními a mezinárodními složkami k zabezpečení jednotného úsilí k minimalizaci ztrát, odstranění následků katastrof, nebo zmírnění nastalé krize.

Pro civilní organizace je také nezbytně nutné komunikovat s dárcovskými a humanitárními agenturami a organizacemi a hlavně také s médii, aby bylo zajištěno včasné varování veřejnosti o nastalé situaci.

Pro zabezpečení takové komunikace je nezbytně nutné zabezpečit nepřetržitý tok informací a rovněž zaručit doručení informace správnému adresátu, v co nejkratším čase a co nejsnazší cestou, k zamezení plýtvání zdrojových prostředků.

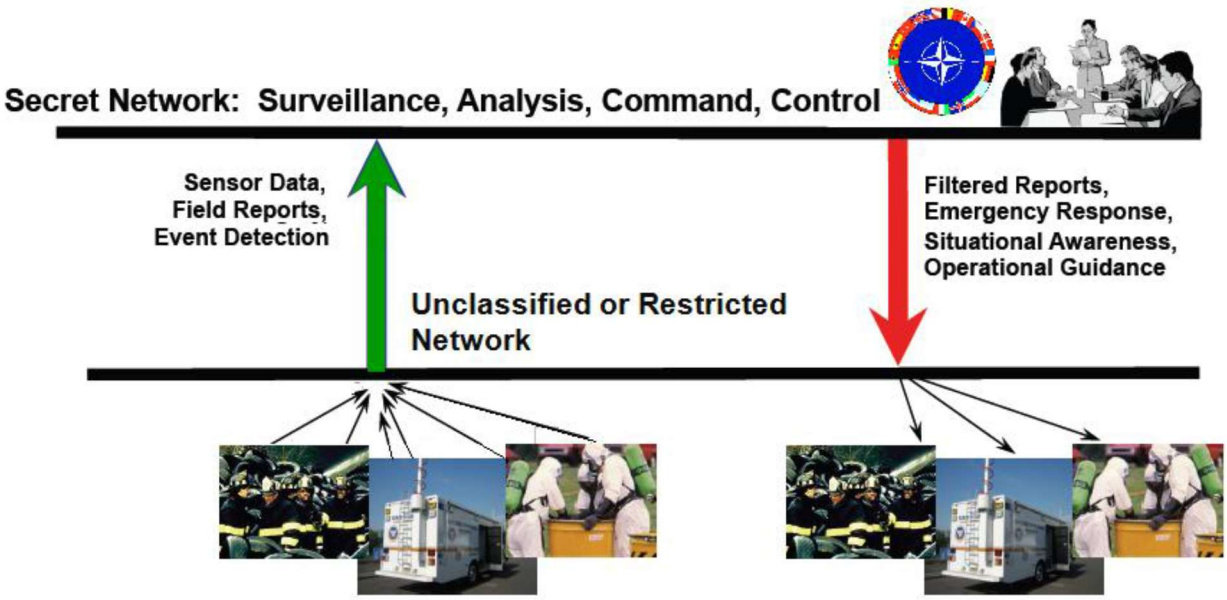
Stále existuje mnoho překážek ve sdílení informací mezi civilním a vojenským sektorem, ať už se jedná o kulturní či mentální rozdíly např. sdílení informací amerického vojenského systému afgánské civilní organizaci, nebo nejsou implementovány mechanismy potřebné k zajištění informačního managementu, odpovídajících bezpečnostních politik a ochrany použité komunikační infrastruktury [1].

Ačkoliv mnoho civilních organizací je vybaveno komerčními technologiemi, o sjednocení standardů, sjednocení typů a provozování komunikace a sjednocení reprezentace dat nemůže být řeč. Téměř každá civilní organizace používá jiné informační a komunikační technologie, a protože jsou nezávislé, nemusí se řídit žádným přijatým standardem, nebo doporučenou politikou zavádění a užívání informačního systému. Jsou používány různé platformy, někdy záleží i pouze na vlastním rozhodnutí, nebo doporučení, případně ceny ve slevové akci.

Sdílení informací vojenského informačního systému do systémů civilních, pak může narazit i na zásadní prvotní problém nekompatibility fyzických rozhraní, a dále na nekompatibilitu na dalších vrstvách ISO/OSI modelu.

Hlavním problémem bezpečného propojení systémů civilních a armádních informačních systémů, však stále zůstávají rozdílné stupně utajení informačních systémů. To je ta nejpodstatnější administrativně-technická překážka zabraňující efektivní výměně dat mezi dvěma systémy. Informace ukládané, zpracovávané a sdílené v doméně civilního informačního systému jsou většinou neutajované, kdežto armádní systémy jsou téměř u všech národů aliance

(28 národů NATO a také 7NNN (non-NATO nations)) utajovány, a to až do stupně Tajné/NATO Secret (viz Obrázek 1).



Obrázek 1 Propojení systémů rozdílného stupně utajení

Většina řešení použitých k výměně dat mezi informačními systémy buď nevyhovuje požadavků na sdílení informací různých stupňů utajení, nebo, se s nimi v podobných systémech ani nepočítá. Ani AČR nemá podobné řešení implementováno a spojení s civilními subjekty buď není realizováno, nebo realizováno tzv. vzduchovou kapsou s následnou kontrolu dat použitého nosiče.

Samozřejmě tento postup je neefektivní, pomalý a naprosto znemožňuje jakoukoliv realizaci výměny dat v reálném čase, nebo blížící se reálnému. Armádní informační systémy disponují např. komponenty přenosu a sdílení polohové informace, komponenty zjišťování, analýzy a hodnocení CBRN situace (Chemical-biological-radioactive-nuclear) a komponenty pro pozorování a hodnocení meteorologické situace a další systémy. Všechny tyto komponenty najdou své uplatnění v rámci spolupráce s IZS, kdy přenos podobné informace může zachraňovat životy [2].

I. TEORETICKÁ ČÁST

2 MOŽNOSTI PROPOJENÍ INFORMAČNÍCH SYSTÉMŮ RŮZNÉHO STUPNĚ UTAJENÍ

2.1 Vyhláška 523/2005 Sb.

Výňatek z vyhlášky č. 523/2005 Sb. situaci objasňuje:

Vzájemné propojení certifikovaných IS lze realizovat, pokud

- je propojení na základě analýzy rizik schváleno v rámci jejich certifikace,
- je mezi nimi realizováno bezpečnostní rozhraní a
- jsou buďto certifikovány pro nakládání s utajovanými informacemi stejného stupně utajení, nebo je propojení realizováno tak, aby bylo zabráněno přenosu utajované informace vyššího stupně utajení, nežli je stupeň utajení, pro který je IS certifikován.

Propojení informačního systému pro nakládání s utajovanými informacemi s informačním systémem pro nakládání s neutajovanými informacemi lze realizovat pouze v případě nezbytné provozní potřeby.

Pokud by nastala nezbytná provozní potřeba pro propojení certifikovaného IS s veřejnou komunikační sítí, pak pouze v případě, že je instalováno vhodné bezpečnostní rozhraní schválené na základě analýzy rizik v rámci certifikace IS tak, aby bylo zamezeno průniku do certifikovaných IS a byl umožněn pouze kontrolovaný přenos dat, nenarušující důvěrnost, integritu a dostupnost utajované informace a dostupnost služeb certifikovaného IS. Zakázáno pro Přísně Tajné.

Z této vyhlášky, která definuje prostředky k realizaci zabezpečení informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi, je pro tento dokument důležitý popis bezpečnostní provozní mód víceúrovňového.

Podle vyhlášky č. 523/2005 Sb. § 7, odst. 5 je popis takového spojení definován takto: *„Bezpečnostní provozní mód víceúrovňový je takové prostředí, které umožňuje v jednom informačním systému současné zpracování utajovaných informací klasifikovaných různými stupni utajení, ve kterém nemusí všichni uživatelé splňovat podmínky přístupu k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být oprávněni pracovat se všemi utajovanými informacemi.“*.

2.2 Legislativní východiska NATO

Obrana ČR je zajištěna aktivní účastí státu v systému kolektivní obrany NATO, rozvojem schopností EU pro zvládání krizí, regionální spolupráci a spolupráci s partnerskými zeměmi.

Armáda ČR se primárně připravuje na obranu území ČR v rámci kolektivní obrany NATO, plnění úkolů ve prospěch společné bezpečnostní a obranné politiky EU a Organizace spojených národů. V případě nutnosti může být zasazena i jako součást ad hoc vytvořené koalice.

V rámci kolektivní obrany a řešení mezinárodních krizí může být AČR zasazována na aliančním území i mimo něj, zpravidla jako součást mnohonárodních sil. Nelze vyloučit její bojové použití na území státu pod národním velením. K prosazování bezpečnostních zájmů ČR může AČR působit i mimo území státu.

ČR jako člen NATO vychází ve svých koncepčních dokumentech ze strategických a legislativních východisek NATO. AČR proto ve svých koncepčních materiálech dalšího směřování rozvoje komunikační a informační infrastruktury, systémů velení a řízení a dalšího rozvoje spojovacího vojska AČR vychází rovněž ze strategických a legislativních východisek NATO.

Řídícími dokumenty pro rozvoj a dosažení interoperability IT sítí a IKT prostředků je dokument AJP-6 (Allied JOINT Publication) pro použití prostředků KIS v rámci spojenecké operace, dále dokumenty CT (Capability Targets), ke kterým se AČR zavázala a jejich plněním bude zabezpečena úroveň interoperability národních sítí vůči sítím koaličním nezbytná pro účelnou a prospěšnou spolupráci v rámci NATO a dalších mezinárodních paktů a uskupení. Dokument NFIP (NATO FMN Implementation Plan) plán pro implementaci konceptu FMN do národního prostředí. Koncept vybudování interoperabilních systémů velení a řízení v rámci NATO, 7NNN (Non-NATO Nations) a PfP (Partners for Peace), který zabezpečí bezešvou výměnu dat mezi aliančními systémy velení a řízení a obsahuje i popis použití zařízení IEG.

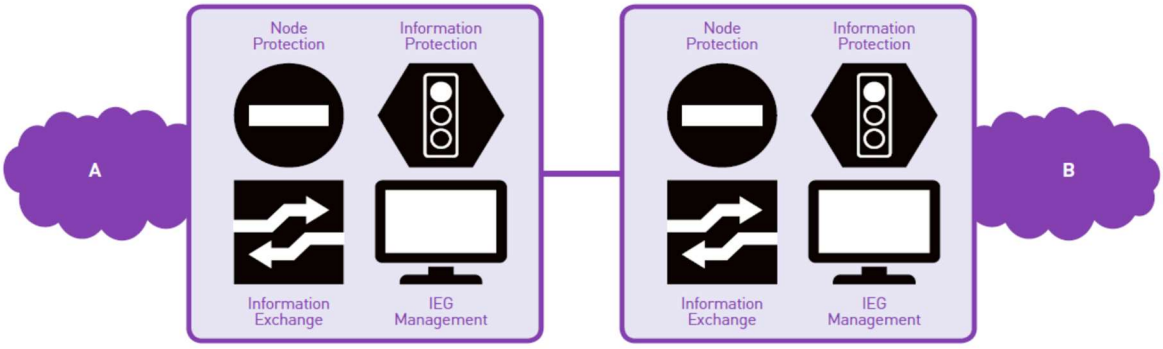
2.3 Bezpečnostní brána IEG

V tomto dokumentu bude popsán systém, který umožňuje bezpečnou výměnu dat mezi heterogenními informačními systémy (jeden vojenského charakteru). Na základě těchto požadavků vyvinuly agentury NATO (NC3A, dnešní NCIA) koncept nasazení tzv. Information Exchange Gateway (IEG). Jedná se o výměnu informací prostřednictvím jediné bezpečnostní entity s jasně definovanými rozhraními a certifikovanými NBÚ (v případě ČR).

Jádrem zautomatizovaného zabezpečení výměny dat mezi vojenským informačním systémem a informačním systémem NGO je tedy prvek IEG. Podobný prvek se v různých obdobách a názvech vyskytuje ve všech odvětvích – bankovní sektor, průmyslová odvětví, vždy však víceméně plní stejnou funkci. Jedná o zajištění bezpečného propojení dvou „cizích“ informačních systémů, které zajistí efektivní sdílení informací a zároveň dodržení všech požadovaných bezpečnostní pravidel. Použitím brány budou kontrolovány datové toky vybraných protokolů vzájemné komunikace. Toto opatření předpokládá implementaci vybraných, schválených a odsouhlasených protokolů (ujednocení) k zajištění možnosti jejich kontroly a umožnění vzájemné komunikace, veškerá další datová výměna nebude zařízením umožněna.

Information Exchange Gateway je systém (bezpečnostní zařízení) navržený k zajištění toku informací mezi sítěmi různého bezpečnostního charakteru (bezpečnostními doménami) za současné dodržení ochrany vnitřní domény od rizik vnějšího napadení systému a ohrožení viry či malwarem. Zařízení zároveň poskytuje ochranu proti vnitřnímu napadení – úniku dat ze systému. IEG obsahuje mnoho bezpečnostních komponent implementovaných do DMZ

(demilitarizované zóny). Brána IEG schovává vnitřní doménu před vnějším světem a propaguje pouze ta rozhraní, která jsou nezbytně nutná pro zajištění přenosu dat, nebo jsou schválená (dohodnutá) pro výměnu dat. I když je IEG implementováno mezi dvě bezpečnostní domény stejného stupně utajení, i tak existuje vzájemná nedůvěra a je nutné instalovat dvě brány, každá chránící svou doménu a konfiguračně vzájemně propojené (Obrázek 2 Zapojení

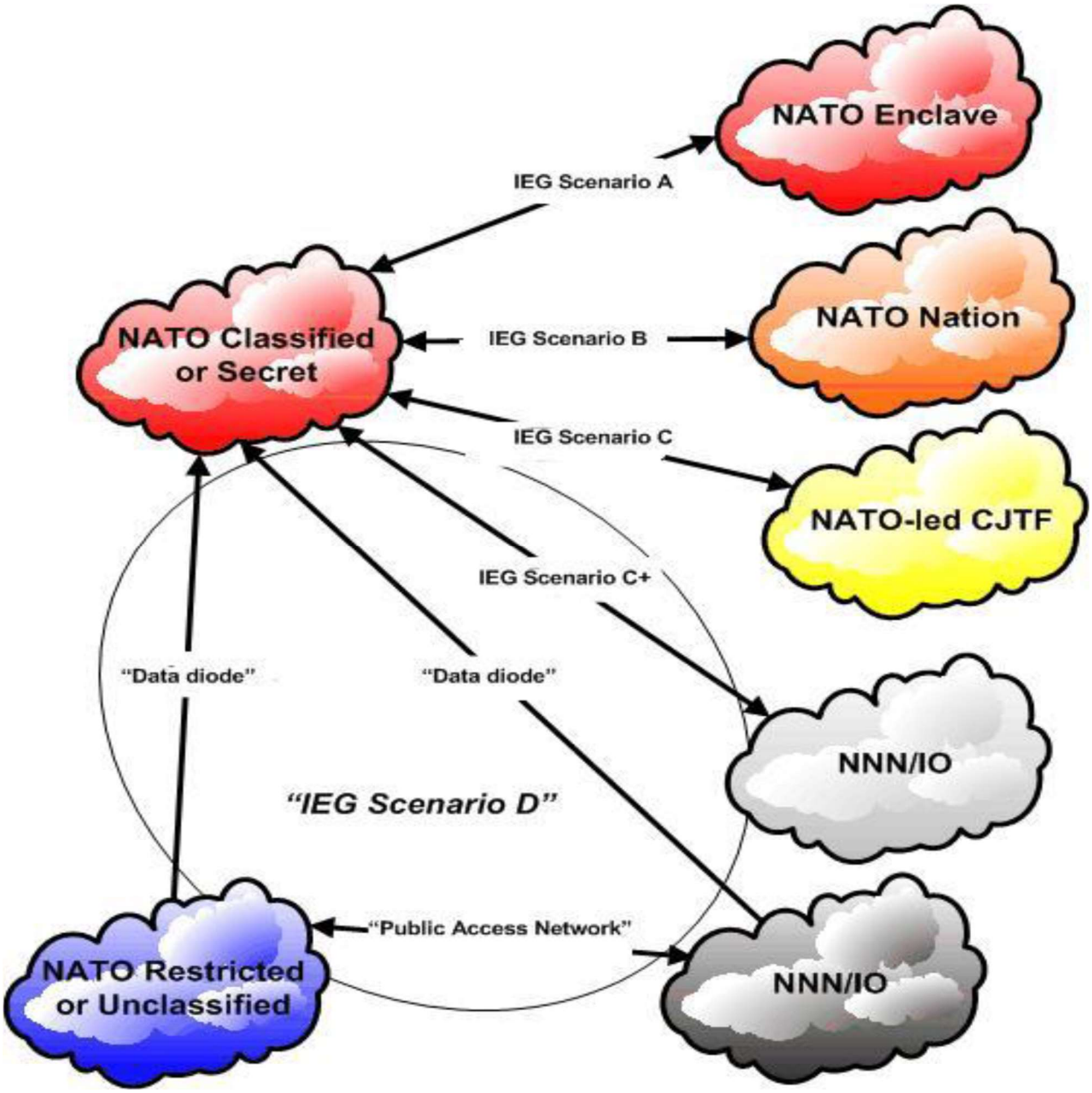


IEG) [3].

Obrázek 2 Zapojení IEG

U bezpečnostních domén NGO není použití stejného nebo vyššího stupně utajení jako v případě vojenských bezpečnostních domén reálné, proto nebude tento scénář uvažován.

Možné scénáře zapojení prvků IEG, dle definice NATO IEG:



Obrázek 3 Scénáře zapojení brány IEG

- **Scénář A** – definuje propojení dvou domén, které mají stejný stupeň utajení a rovněž stejný typový informační systém NATO. Jedná se o bránu, která je určena k provozování a propojování dvou informačních systémů NATO, provozovaných různých velitelstvími, organizacemi, nebo agenturami NATO. Typicky užíváno pro provoz NATO enklávy v síti NATO národů. V podmínkách AČR se jedná o provoz informačních systémů NATO dislokovaných na českých národních velitelstvích.
- **Scénář B** – definuje propojení dvou domén, které mají stejný stupeň utajení, ale rozdílné bezpečnostní politiky a provozně-bezpečnostní směrnice. Jedná se propojení národních systémů velení a řízení do systémů NATO. Tento scénář pokrývá i možnosti propojení více informačních systémů řízených stejnou bezpečnostní politikou,

ale různého stupně utajení – v rámci NATO spojení dvou informačních systémů NATO SECRET a NATO RESTRICTED – řízených jednotnou bezpečnostní politikou NATO.

- **Scénář C** – definuje propojení informačních systémů nasazení v poli (v operaci) proti systémům stacionárním (scénáře A a B)
- **Scénář D** – definuje propojení informačních systémů NATO (nebo odpovídajících národních systémů velení a řízení) a systémů mezinárodních organizací, nebo NGO (civilních organizací).
- **Scénář E** – definuje připojení NATO (nebo odpovídajících národních systémů velení a řízení) do internetu, nebo jiných systémů s přímým propojením do internetu.

V případě spolupráce s civilní organizací nebo agenturou je z vojenského hlediska uvažován typ propojení IEG-D. Rozdíl mezi scénáři D a E je v použití základního zabezpečení ve formě použití firewallu, antivirové a mallware ochrany a dalších základních bezpečnostních opatření. Scénář E je považován za přímé ohrožení systémů bez jakékoliv ochrany. Samotné zařízení IEG-D je v podstatě datová dioda neumožňující obousměrnou komunikaci, v poslední době se však tato architektura začíná měnit a to zejména s nástupem nových technologií, jako je Data Labelling – bezpečnostní značkování dat a jejich kontrola [4].

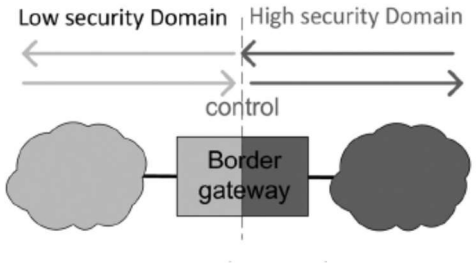
V moderní výpočetní technice existují způsoby a řešení k zajištění bezpečné výměny dat různého stupně utajení, jsou to však řešení určená pouze specificky pro jeden protokol (např. web service guard, mail guard apod.). Universální řešení nabízí filtrování a kontrolu prostřednictvím protokolu XML.

Běžně komerčně dostupné řešení (COTS, Commercail-of-the-shelf) nabízejí kontrolní mechanismy na základě protokolu XML pro kontrolu webového rozhraní, většinou nazývány XML gateway (např. XML Firewall společnosti IBM). Poskytují autorizaci oprávněným uživatelům webu na základě implementované bezpečnostní politiky.

Běžně se na branách IEG používají komerčně dostupné kontrolní mechanismy. Brány pak dokáží poskytovat zabezpečený přenos dat v cross-domain prostředí a kontrolovat propouštěná data na základě bezpečnostních politik, ale stále pro jeden jediný zvolený protokol. Jedná se o neprovázané funkcionality. Není běžně dostupný software (guard) zajišťující úplnou kontrolu všech příchozích protokolů a výstupů aplikací.

Civilní a armádní informační systémy se liší v zásadních bodech: bezpečnostní nastavení a opatření, implementovaná bezpečnostní politika a stupeň utajení. Realizace spojení systémů s vyšším a nižším stupněm utajení je od možná na základě popisu dle vyhlášky 523/2005 Sb. Aby bylo zabráněno přenosu utajované informace vyššího stupně utajení, nežli je stupeň utajení, pro který je informační systém certifikován je nutné implementovat opatření daná

touto vyhláškou (datová dioda). Pro umožnění efektivní výměny dat je však nutné umožnění komunikace obousměrné (Obrázek 4 Filosofie spojení Low-High domén).



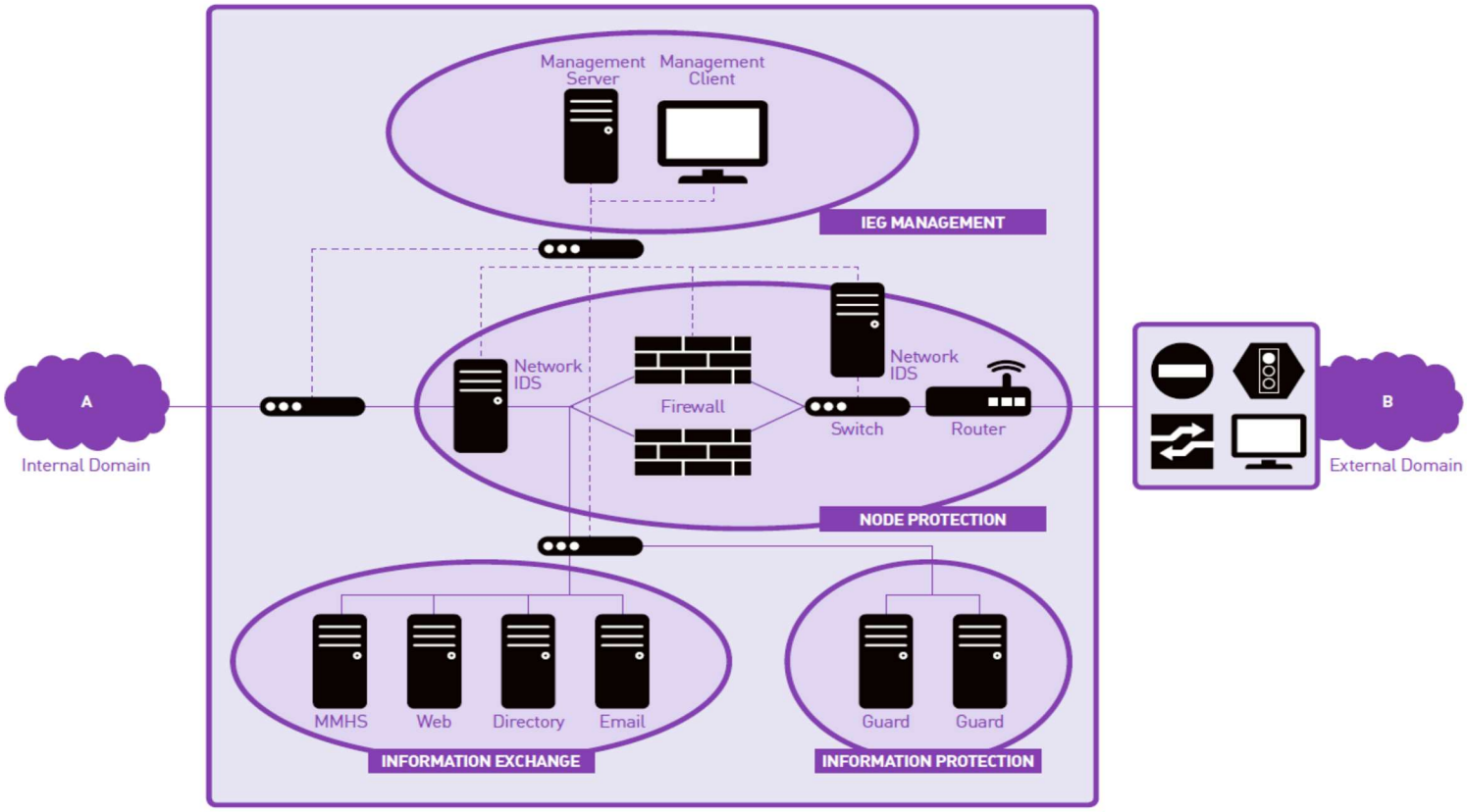
Obrázek 4 Filosofie spojení Low-High domén

2.4 NATO Referenční architektura IEG

Pro základní funkci bran IEG byly ze strany NATO vydefinovány čtyři základní ochranné prvky. Prvky jsou postupně přidávány, tak aby naplnily a pokryly všechny uváděné scénáře použití bran IEG dle Obrázek 3.

Základní moduly bran IEG:

- Node Protection – ochraňuje infrastrukturu chráněné domény a to nástroji jako jsou network a packet filtering, intrusion detection a virus a mallware ochrana.
- Information Exchange – účeleme tohoto ochranného prvku je zabezpečení výměny informaci s jinými doménami. Tok informací je kontrolován a IEG používá proxy k zabezpečení výměny pouze specifických a schválených informací. Tento typ ochrany rovněž zabezpečuje tok dat v lokálních či jiných neroutovaných sítích, kde není možné využívat pravidel nastavených směrovačem (např. i rádiový přenos).
- Information Protection - tento prvek ochraňuje data uvnitř domény a poskytuje prvky služby k ochraně kontroly propustnosti dat mimo systém, zabránění případnému úniku dat.
- IEG Management – vlastní interní management brány IEG. Oddělená samostatná ne-propustná síť pro zabezpečení nastavení bezpečnostních pravidel brány [5].



Obrázek 5 NATO Referenční architektura IEG

Ochranné prvky brány IEG podrobný popis

1. Node Protection

   Infrastruktura IEG je chráněna za použitím síťových zařízení, komponent, řešení a aplikací tuto ochranu umožňující:

   - Router

   Router zabezpečuje síťové směrování a volitelně také NAT (Network Address Translation), bezpečnostní mechanismus umožňující úpravy síťového provozu přepisem zdrojové nebo cílové IP adresy. Dále provádí packet filtering k zabezpečení alespoň základní ochrany proti škodlivému provozu z vnější sítě. Router je jediný prvek, který na bráně IEG propaguje svou adresu a jeho úkolem je skrýt celou vnitřní doménu od okolního síťového prostředí.

   - Switch

   Switch slouží k zabezpečení spojení interních komponent brány IEG. Ačkoliv moderní switche již poskytují také mnoho ochranných a zabezpečovacích mechanismů, ať je už je to ochrana a zabezpečení portů, funkce vázání na adresu IP,

MAC, port, VID, ACL, ochrana proti DoS, kontrola všesměrového vysílání, DHCP Snooping, ověřování 802.1X a protokol Radius.

- Firewall

Firewall, nejčastěji zapojený ve failover módu, zabezpečuje kontrolu protokolů a propouští pouze informace povolené bezpečnostními politikami. Firewall je jediné zařízení, které vytváří spojení (propojení) s jiným systémem. Veškerý provoz s cizí sítě projde nejprve tímto zařízením. I konstrukce a použití zařízení firewall udělal vývojový skok vpřed. Dnes již běžně používané NextGeneratins firewally, dokáží vedle svých běžných funkcí kontrolovat i provoz na dalších vrstvách ISO/OSI modelu.

- Instrusion Detection System

Intrusion Detection systém chrání infrastrukturu detekování nežádoucího provozu. Detekce je prováděna (zachytávána) na předem rozmístěných zařízeních (sondách), které monitorují provoz a okamžitě hlásí administrátorovi, či jinému dohledu, narušení sítě – odchýlení od předem definovaných bezpečnostních pravidel. Network based IDS (NIDS) prověřuje síťový provoz vstupující do brány IEG a chrání systém proti potencionálnímu skenování portů, nebo útokům odepřením služeb (DoS – Denial of Services). NIDS mohou být rovněž použity pro zabezpečení provozu na vnitřní doméně při pokusu o vnitřní napadení sítě (Insider Attack). Host based IDS (HIDS) jsou zařízení, která ve spolupráci s NIDS monitorují jednotlivé počítače (tam, kde jsou nasazeny) a hlásí nepatřičné chování, nebo neautorizované přístupy ke zdrojům dat. Provoz systému IDS vyžaduje aktivní management, tzn. stálý dohled a analytické a vyhodnocovací pracoviště. Ke správné funkcionalitě požaduje rovněž periodickou aktualizaci signatur k rozpoznání útoků, nebo nestandardního provozu.

Pozn. Systém CIS Security skládající se z podsystémů Cyber Defense a Information Assurance vydá na samostatnou BP.

- Information Exchange

Systém výměny informací mezi doménami je povolen pouze za použití proxy serveru, což je prostředník, který může analyzovat obsah komunikace. Tyto servery zajišťují, že žádná informace se přímo nedostane do datových toků uvnitř vnitřní domény. Proxy servery zajistí, že spojení bude provedeno pouze s autorizované vzdálenými zdroji a jsou používány techniky jako autentizace a vztahy důvěryhodnosti. Proxy servery rovněž zajišťují základní úroveň ochrany detekcí a počet proxy serverů v systému se liší na základě definice vyměňovaných informací – co vše je třeba sdílet, má vlastní proxy server. Každá služba potřebuje vlastní proxy server k zajištění datového toku mezi doménami. Běžně jsou v branách zabezpečovány základní služby – email, web browsing, directory replication a military messaging (vojenské formalizované zprávy – hlášení situace, povely, signály apod.).

- Information Protection

Služby informačního zabezpečení jsou poskytovány ochraňujícími systém na aplikační úrovni (tzv. guardy). Guardy aplikací prozkoumávají data aplikací k zabezpečení, že daná informace „je způsobilá“, schválená k opuštění prostředí vnitřní domény. Bezpečnostní politika definuje co „být způsobilý“ znamená a aplikační guard poté tuto politiku aplikuje v praxi. Typicky je zjišťováno kým je informace poskytnuta, kdo je adresátem, jaký je typ informace a nejdůležitější prvek – zda má informace odpovídající bezpečnostní značku. Aplikační guardy také dokáží poskytovat ochranu infrastruktury (Node Protection) a to zajištěním, že příchozí data neobsahují žádné viry ani mallware či jiný škodlivý kód. Brána IEG poskytuje v základním provedení tyto guardy:

- Messaging Guard k zabezpečení emailové a jiné komunikace (zabezpečení kontroly služeb human-to-human interaction). Messaging Guard ke kontrole a potvrzení správnosti a úplnosti informace provádí kontrolu:
  - Platné bezpečnostní značky (Security Label) – k zabazpečení, že ke zprávě je připojena značka ve správném formátu (pro emailovou zprávu obvykle umístěná v hlavičce)
  - Bezpečnostní značku pro možné opuštění vnitřní domény – k zabezpečení, že značka ve zprávě opravňuje aplikaci zprávu poslat mimo vnitřní doménu
  - Platnou přílohu – k zabezpečení, že zpráva je posílána pouze s povoleným typem příloh
  - Platného odesílatele/adresáta – k zabezpečení autentizace a důvěryhodnosti zdroje a příjemce.
- Instant messaging Guard – k zabezpečení textové komunikace (chat)
- Služba directory replication – k zabezpčení kontroly úplnosti a správnosti provedení replikace adresářových služeb (odhalení potenciální podvrhu nastrčeného uživatele) – nutná aplikace mechanismu replikace používajícího formát XML
- Služby web services – zabezpečení kontroly úplnosti, správnosti a integrity dat ve formátu XML

XML guardy validují XML schéma a kontrolují bezpečnostní značky založené na XML formátu a jsou předmětem této práce.

- IEG Management

  Vlastní interní management brány IEG. Oddělená samostatná nepropustná síť pro zabezpečení nastavení bezpečnostních pravidel brány za použití SNMP protokolu [6].

Referenční architektura IEG předpokládá implementaci kontrolních mechanismů na zařízení IEG. Je poté umožněna kontrola veškerých příchozích informací a na základě nastavených politik také kontrola informací odchozích. Kontrolní mechanismy (guardy) pro různé protokoly, formáty a aplikace jsou implementovány do jednoho hraničního zařízení, kde jsou poté filtrovány různé druhy informací dle použitých protokolů a aplikací. K realizaci tohoto způsobu nasazení je potřeba použít sjednocený postup reprezentace dat, jednotné postupy nasazení všech kontrolních mechanismů a jednotné metody jejich běhu na zařízení, aby nebyly vzájemně ovlivňovány či, aby kontrolním mechanismem nebyly narušeny, nebo pozastaveny interní funkce samotného zařízení IEG.

Referenční architektura navrhuje použití protokolů SOAP/XML pro jednotnou reprezentaci dat v kontrolních mechanismech zařízení IEG. Zařízení IEG poté realizuje rozhodovací proces, ve které bude určeno pro každý příchozí typ dat, jak s ním bude naloženo a kam bude předán.

Pro správné předání informace musí zařízení rozhodnout na základě těchto vstupních dat:

- zdroj a cíl informace
- bezpečnostní značka (security label) informace
- bezpečnostní politika pro specifický druh výměny informací

Lze vyměňovat pouze informace, pro které:

- zdroj i cíl jsou jasně identifikovatelné entity v systému
- bezpečnostní značka byla potvrzena třetí stranou (autoritou) a je zajištěna integrita dat
- bezpečnostní politika dovoluje odeslání informace na základě stupně utajení a uživatelských práv.

Zařízení IEG musí být schopno kontrolovat kompletní datový provoz mezi doménami. Musí být schopné rozpoznat protokoly a rovněž filtrovat nepovolené pakety dat na základě TCP/IP filtru paketů. Musí být obsaženy prvky IDS (Intrusion Detection System) a IPS (Intrusion Prevention System) pro příchozí i odchozí datový provoz. Kontroly probíhají na síťové vrstvě. Zařízení IEG musí být schopno analyzovat obsah přenášených dat, pro tyto účely má implementovány mechanismy kontrolu virů a malware.

Tato práce se dále bude zabývat implementací jednoho dílčího mechanismu kontroly dat zařízení IEG, a sice Messaging Guard a jeho bezpečnostními dílčími částmi – mechanismem bezpečnostního značkování dat. Mechanismus bezpečnostního značkování bude v této rozpracován bez ohledu na ostatní služby zařízení IEG a nebude brána jejich vzájemná podpora

a integrace. Mechanismus bezpečnostního značkování dat bude posuzován a použit jako samostatný a bude provedena jeho integrace do stávajícího informačního systému bez ohledu na jiné zabezpečovací mechanismy.

2.5 Dílčí závěr

Propojení informačních systémů různého stupně utajení lze realizovat pouze za použití speciálního zařízení, které umožní celkovou kontrolu všech příchozích i odchozích dat, zajistí integritu systému, jednoznačně identifikuje a autentizuje uživatele informačního systému, zajistí ochrana důvěrnosti a integrity autentizační informace. Dále umožní volitelné řízení přístupu k objektům informačního systému na základě přístupových práv uživatele.

Zařízení musí poskytovat nepřetržité zaznamenávání bezpečnostně relevantních událostí do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením.

Vývoj podobného zařízení je značně nákladná záležitost a zařízení komplexně pokrývající všechny potřeby a všechny módy komunikace vojenského systému není na trhu běžně dostupné. I pokud je dostupná mezinárodní referenční architektura, nadále je nutné přizpůsobení národním potřebám. XML guardy navržené v referenční architektuře jsou definovány pouze obecně pro základní služby human-to-human interakce, pro spojení např. s IZS je nutná dodatečná definice formalizovaných zpráv předávaných do vojenského systému a definice všech dalších nestandardních dat přicházejících do IS a poté jim guardy přizpůsobit.

3 BEZPEČNOSTNÍ ZNAČKOVÁNÍ DAT

3.1 Bezpečnostní značkování dat v podmínkách vojenských systémů velení a řízení

Historicky jsou vojenské systémy velení a řízená chápány jako system-centric, tzn., že informační systém je chápán jako uzavřený celek s vlastní hierarchií vnitřních prvků a jeho interakce s okolím jsou zabezpečovány pouze na jeho vnějších rozhraních. Vnitřní procesy a postupy nejsou známy, zveřejňovány a připojeným dalším informačním systémům (bezpečnostním doménám) je známo pouze vnější rozhraní a typ vstupně-výstupních dat.

Dalším vývojovým krokem ve změně chápání informačních systémů byl přechod k oblasti network-centric. Smyslem bylo síťově propojit veškeré periferie, senzory, palebné prostředky, průzkumné prostředky, operátory, administrátory, velitele a další možné entity. Vše propojeno bez hierarchie na jedné horizontální úrovni. Systém už nebyl jeden celek tvořený pouze komunikačními a informačními prostředky, ale stal se bezpečnostní doménou zahrnující všechny entity. Tento přístup umožňoval rychlejší komunikaci všech entit, bez schvalovacích procedur (tam kde je to možné), bez nutnosti zajištění prostupu nadřízeným velícím prvkem. Zajištění vzájemné komunikace cizích nižších jednotek (družstva, malé týmy) mezi sebou nebylo obvykle prováděno na horizontální úrovni. Původní cesta komunikace system-centric přístupu byla striktně vertikální. Podřízený navázal komunikaci nebo poslal zjištěnou informaci nadřízenému prvku a ten poté teprve zajistil distribuci informace ostatním jednotkám vojenského uskupení nebo svými prostředky zajistil požadovanou komunikaci. Novým přístupem byla umožněna rychlejší efektivní komunikace malých podřízených jednotek cizích států na jednom bojišti bez nutnosti zajištění komunikace až vyššími velícími prvky často umístěnými geograficky daleko od sebe.

Mechanismus bezpečnostního značkování dat nachází své uplatnění v nejnovějším přístupu chápání informačních systémů velení a řízení, a sice data-centric. Poučení z použití vojenských systémů velení a řízení v operacích indikovalo závažné nedostatky zejména v nákladech vynaložených na cenu, investice, provoz a správu network-centric systémů. Navíc použitá architektura oddělených bezpečnostních domén neumožňuje rychlé a efektivní sdílení dat na moderním bojišti. Použití utajovaných systémů pro národní účely např. krizového řízení je v současné době téměř fikcí a jediný možný přenos je vzduchovou kapsou (air-gap), a to právě z důvodu rozdílných stupňů utajení informačních systémů. Nejsou naplněny základní podmínky vedení bojové operace „need-to-know“ a „need-to-share“ (mít všechny potřebné informace k vydání rozkazu a mít schopnost poté rozkaz a další data vydat (sdílet)).

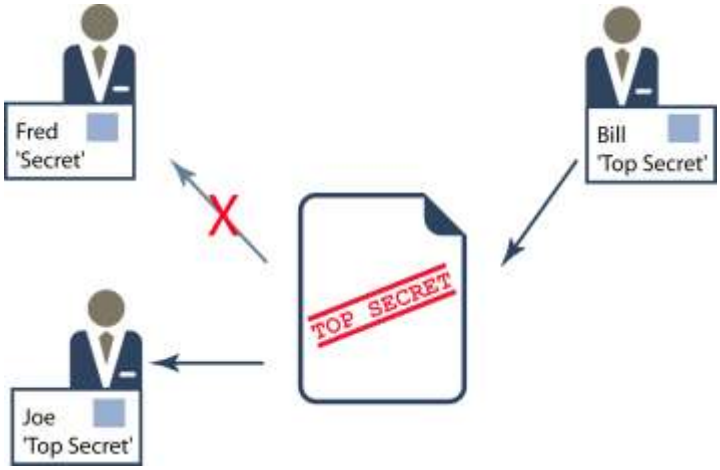
3.2 Popis bezpečnostního značení

3.2.1 Jak bezpečnostní značky fungují (značení dokumentů)

Základní mechanismus značkování zpráv je známý většině lidí. Dokumenty jsou označeny (tiskem, polepkou) klasifikací, např. „Vyhrazené“, „Důvěrné“, „Tajné“. Tato značka musí být viditelná na dokumentu.

Lidé, kteří mají odpovídající prověření, poté mohou mít přístup k odpovídající dokumentaci. Např. pro osobu se stupněm prověření „Tajné“ je dostupná dokumentace stupně „Tajné“, ale již nemá přístup k dokumentaci stupně „Přísně tajné“.

Bezpečnostní značky na dokumentech jsou jen jedním aspektem modelu, jak mohou být značky připojeny k informaci. Bezpečnostní značku může mít v informačním systému i role, nebo osoba. Osoba může být označena jako „Tajné“, poté se seznamuje se zprávami dle Obrázek 6.



Obrázek 6 Neelektronická klasifikace osob a dokumentů

Jádrem bezpečnostního značkování dat je model: osoba (přistupující k informacím) má prověření, které kontroluje oprávněnost přístupu. Na Obrázek 6 je tato situace znázorněna. Bill je tvůrce (nebo odesílatel) dokumentu s označením „Top Secret/Přísně tajné“. Ověřuje prověření spolupracovníků Joea a Freda. Předává dokument Joeovi s odpovídajícím prověřením, ale Fredovi je přístup k dokumentu zamítnut.

Bezpečnostní prověření může být také asociováno na lokalitu. Např. jednací místnosti mohou být označeny jako „Tajné“, jsou poté používány a autorizovány k diskuzi nad tajnými informacemi, ale nemohou být použity k probírání „Přísně tajných“ témat, v souladu se základním modelem bezpečnostního značkování.

3.2.2 Proč je užíváno bezpečnostního značkování

Bezpečnostní značkování je široce rozšířený mechanismus pro kontrolu přístupu k informacím, a to z mnoha důvodů:

1. Model bezpečnostního značkování dat/dokumentace je jasný a je velmi snadné jej pochopit (polepky apod.), tento fakt je velmi důležitý, čím je systém komplexnější, tím je náchylnější k chybě (uživatele/systému).
2. Prověření a klasifikace může být spravovány větší skupinou lidí, zaměstnaných v různých organizacích (správa většího archivu z více míst, správa sdruženého toku informací více organizací).

3. Další přístupy klasifikace dat/dokumentů nebudou tolik praktické, zejména tam, kde je žádán přístup většího počtu lidí k různým částem archivu s různou klasifikací jeho částí. Je poté nutné dodržovat:
    a. Udržovat povědomí o každém dokumentu, kdo má přístup,
    b. Pro každého uživatele zaznamenat, kam má přístup a proč,
    c. Udržovat nezávislý seznam k zabezpečení porovnání uživatele a dokumentu.

    Tyto atributy poskytuje systém bezpečnostní značkování dat/dokumentů a je ověřen praxí.

3.2.3 Co je bezpečnostní značka

Nejdůležitější část, a občas také jediná část bezpečnostní značky, je stupeň utajení/klasifikace informace. Mnoho vlád, vládních úřadů, armád a organizací používá stejné stupně klasifikace:

- Unclassified/Neutajované,
- Restricted/Vyhrazené,
- Confidental/Důvěrné,
- Secret/Tajné,
- Top Secret/Přísně tajné.

Toto je doporučené/nařízené schéma, je z něj patrné, že kdokoliv se stupněm prověření „Tajné“ může přistupovat k informacím „Tajné/Důvěrné/Vyhrazené/Neutajované“, ale již ne „Přísně tajné“. Toto značení stupně utajení je universální a mezinárodní.

Jiným přístupen ke značkování dat může být implementace bezpečnostní značek dle RFC 3114. V RFC použitý příklad korporace Amoco definuje vlastní sadu bezpečnostních značek platných pouze pro danou korporaci, např.: “Amoco-general“, „Amoco-confidental“ a „Amoco-highly-confidental“.

Nastávají i situace kdy stupně klasifikace nedostatečně přesně oddělují stupně citlivosti informace. Aby bylo dosaženo lepší kontroly informací je možné do bezpečnostní značky přidat další dodatečné informace, známé jako kategorie, např.:

- Bezpečnostní značky jsou často používány vzhledem k národní bezpečnosti. Kategorie národů je často používána pro zajištění kontroly informací vzhledem k ná-

rodní bezpečnosti. Je možné také zabezpečit sílení informací pouze vybranými národy, např. označením „US-UK-two-eyes“ znamenající sdílení informací pouze v omezeném okruhu národů.

- Armády, agentury a organizace NATO naopak potřebují kontrolovat informace podle tématu. Např. kategorie „Biologické zbraně“ je použita pro omezení přístupu k informacím pouze osobám prověřeným pracovat s těmito informacemi, ale ne všem s odpovídajícím bezpečnostním prověřením [7].

Známe tři typy kategorií:

1. Restrictive. Uživatel musí být prověřen a splňovat všechny údaje uvedené ve značce. Tato kategorie je vhodná pro možnost implementace dodatečných kontrolních mechanismů (zpřesňující informace o přístupu k informacím) a užívá se pro striktní zamezení přístupu pro neautorizované osoby.
2. Permissive. Uživatel musí být prověřen a splňovat alespoň některý údaj uvedený ve značce. Tato kategorie je užívána zejména pro informace sdílené více národy (uvedených ve značce) a uživatel musí být příslušníkem jednoho z nich (alespoň jeden údaj ve značce).
3. Informative. Kategorie mající informativní charakter pro uživatele, ale není kontrolována a kontrola dle této kategorie není vyžadována.

Sama kategorizace bezpečnostních značek může být klasifikována, tzn., že hodnoty ve značce určené pro porovnání mohou být sdíleny také pouze v odpovídajícím zabezpečeném prostředí.

3.2.4 Kontrola bezpečnostních značek a prověření

Dokument nebo informace s implementovanou bezpečnostní značkou je vytvořena osobou/uživatelem s odpovídajícím prověřením. Klíčová kontrola probíhá, když je dokument nebo informace odesílán jinému uživateli/osobě. Má-li druhá osoba odpovídající prověření, pak je informace předána.

Porovnávání bezpečnostních značek a bezpečnostního prověření je jednoznačné. Problémem je však určení klasifikace informace tvůrcem informace. Ten musí vzít v potaz bezpečnostní prověření příjemce zároveň s obsahem informace. V mnoha organizacích s vyšším stupněm utajení jsou zaměstnanci vybaveni visačkami s viditelnou fotografií, jménem a bezpečnostním prověření (většina barva celé visačky). Návštěvník v takové organizaci musí být prověřen (doložit bezpečnostní prověření) organizací, která je důvěryhodná (v ČR NBÚ). Před příjezdem je nutné předložit bezpečnostní prověření bezpečnostnímu důstojníkovi/úředníkovi, který porovná oprávnění vstupu do požadovaných prostor s údaji na bezpečnostním

prověření a vstup povolí nebo nikoliv. Při vstupu návštěvy vydá bezpečnostní visačku s barevným odlišením pro označení návštěvy. Tyto proces jsou v mechanismech bezpečnostního značkování dat a jejich použití v praxi pouze použity v elektronické podobě. Detaily podobných procesů se mohou lišit, ale je jasně viditelné, že nejdůležitější a nejkomplexnější částí procesu je kontrola a porovnání bezpečnostního prověření a bezpečnostní značky dat/informací, ke kterým je přistupováno.

3.2.5 Bezpečnostní Politika

Bezpečnostní politika je obecný pojem. V kontextu s mechanismem bezpečnostního značkování dat má bezpečnostní politika dvě hlavní vlastnosti:

1. Bezpečnostní Politika definuje hodnoty jednotlivých částí a kategorií bezpečnostní značky, které jsou poté platné a jsou verifikovány,
2. Bezpečnostní Politika definuje, jak jsou bezpečnostní značky porovnávány oproti bezpečnostnímu prověření uživatele.

Termín Bezpečnostní Politika je použit pro zpřesnění výrazu bezpečnostní politika. Jedná se o užší vyjádření bezpečnostních pravidel v kontextu použité obecné politiky s daleko širším záběrem. Je to právě Bezpečnostní Politika, která se liší mezi národy a organizacemi. Různé organizace mají různé Bezpečnostní Politiky vycházející z obecné bezpečnostní politiky.

Bezpečnostní Politika definuje, které úrovně klasifikace informací jsou platné a také jejich hierarchii a definuje rovněž kategorie bezpečnostních značek.

Aplikace provádějící kontrolu bezpečnostního značkování musí provádět dvě úrovně kontroly:

- Kontrolu syntaxe k oddělení bezpečnostní značky a k identifikaci Bezpečnostní Politiky,
- Porovnání bezpečnostní značky a bezpečnostního prověření uživatele oproti Bezpečnostní Politice.
- Dodatkem je prováděno také ověření platnosti bezpečnostní prověření uživatele.

Bezpečnostní prověření uživatele je prováděno analogicky jako ověření bezpečnostních značkování. Tyto funkce má přístupový kontrolní a rozhodovací mechanismus (XML Guard).

3.2.5.1 Jak zobrazovat bezpečnostní značky

Bezpečnostní značky jsou užívány v mnoha aplikacích informačního systému, to jak jsou zobrazeny uživateli, zajišťuje konzistenci reprezentace ochrany dat a také předchází zmatení uživatele. Možné způsoby:

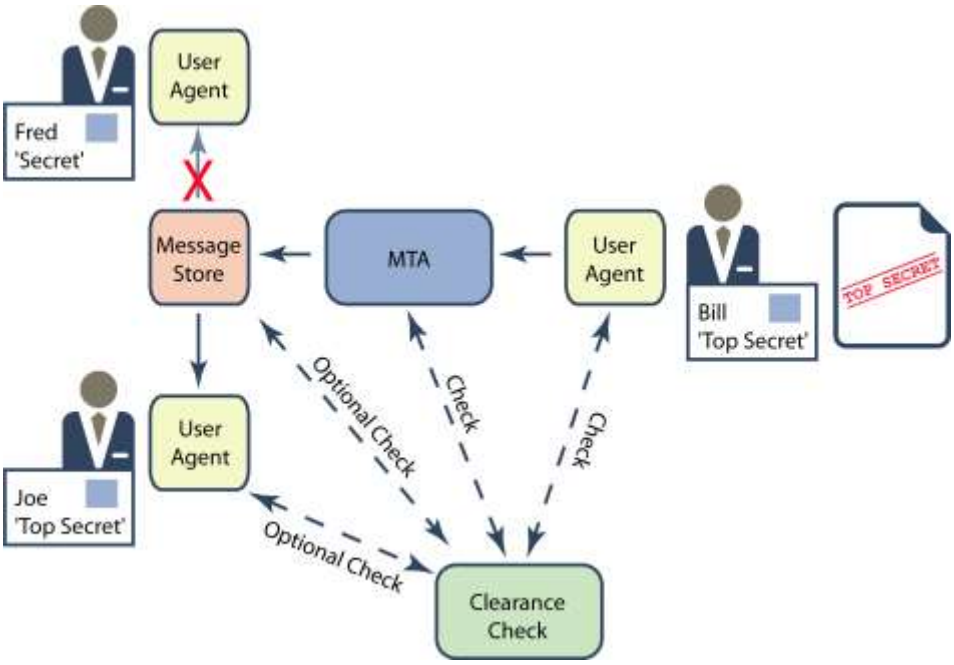
- Text v úvodu dokumentu (jiný na závěr dokumentu),
- Text na horní straně každé strany,
- Barevné odlišení.

3.2.6 Proč jsou bezpečnostní značky užitečné

Hlavním cílem pro použití bezpečnostního značkování je podpora organizace, která používá klasifikované dokumenty a má zaměstnance s bezpečnostním prověřením, kteří k nim přistupují. Bezpečnostní značky jsou aplikovány na všechny informace. Je-li informace elektronická a má se posílat prostřednictvím informačního systému, pak je použit stejný mechanismus jako v případě neelektronického použití na dokumentech. Je-li informace zpracovávána elektronicky, je nutné, aby informační systém byl schopen vynutit použití bezpečnostních politik a zajistit, aby klasifikovaná informace nemohla být poslána uživateli bez odpovídajícího prověření. Primární účelem bezpečnostního značkování je tedy roztřídění informací dle klasifikace.

Bezpečnostní značkování a bezpečnostní prověření poskytuje mechanismus kontroly přístupu k informacím, který funguje dobře i pro velkou skupinu uživatelů. Je to efektivní přístup k řešení ochrany informací v elektronické podobě.

Následující obrázek zobrazuje předcházející situaci sdílení dokumentu tentokráte v elektronické podobě. Bill vytvořil dokument s klasifikací „Top Secret/Přísně tajné“. Joe má bezpečnostní prověření „Top Secret/Přísně tajné“ a může přijmout dokument. Fred má bezpečnostní prověření pouze „Secret/Tajné“ a dokument přijmout nesmí.



Obrázek 7 Elektronická klasifikace osob a dokumentů

Kontrola přístupu k elektronickému dokumentu založené na aplikované Bezpečnostní Politice se projeví v následujících místech informačního systému:

1. Billův User Agent (UA) – řízení osobní politiky uživatele. UA zjistí zamýšlené příjemce zprávy a porovná bezpečnostní značku dokumentu s bezpečnostním prověřením příjemce. Tím bude zajištěno, že UA odešle dokument odpovídajícímu příjemci.
2. V MTA (Message Transfer Agent). Message Transfer Agent také provádí základní kontrolu. Komunikační prostředí pro přenos zpráv není zcela odkázáno jen na chování uživatele. Doručuje však pouze základní porovnání, že je případný problém v rozporu mezi bezpečnostní značkou a bezpečnostním prověřením, ale dále situaci neřeší.
3. Message Store – úložiště zpráv. Provádí kontrolu bezpečnostní značky a bezpečnostního prověření uživatele před uvolněním informace příjemci.
4. UA příjemce. UA příjemce provádí rovněž kontrolu bezpečnostní značky a odpovídajícího bezpečnostního prověření uživatele a uživateli jsou zobrazeny pouze schválené zprávy/informace.

Kontrola bezpečnostní značky oproti bezpečnostnímu prověření uživatele tedy probíhá na více místech informačního systému [8].

3.2.7 Elektronická reprezentace bezpečnostní značky

3.2.7.1 Požadavky na online reprezentaci značky

Hlavní část schématu bezpečnostní značky je formát, který použit pro reprezentaci bezpečnostní značky. Online reprezentace bezpečnostní značky musí splňovat:

1. Musí být použitelná pro širokou škálu protokolů, formátů, včetně dokumentů, emailů, zpráv chatu, adresářových a databázových dat.
2. Musí podporovat širokou škálu formátů Bezpečnostních Politik, nesmí být izolována pouze pro použití v jedné organizaci, ale zajišťovat komunikaci.
3. Musí být kompaktní:
    a. Některé aplikace potřebují označit pouze velmi malou informaci, je nežádoucí, aby bezpečnostní značka byla větší než samotná chránění informace.
    b. Některé organizace, zejména armáda, operují v prostředí se zajištěním velmi nízké přenosové rychlosti – značka musí být použitelná i v takovém prostředí.
4. Musí být integrovatelná spolu s digitálním podpisem.

3.2.7.2 Elektronická reprezentace bezpečnostní značky

Bezpečnostní značky jsou obecně specifikovány standardy. Nejvíce rozšířené jsou tyto dva standardy:

1. ESS Security Labels jsou definovány v internetovém standardu „Enhanced Security Services for S/MIME“ (RFC 2634). Tato specifikace je široce rozšířena a splňuje požadavky uvedené výše v textu. ESS Security Labels jsou používány pro S/MIME (standardy pro zabezpečení dokumentů a emailů) a také ve STANAG 4406 (vojenský technický standard Military Messaging pro zabezpečení výměny varovných zpráv) [9].

Ve zbytku dokumentu bude vždy referováno k těmto dvěma standardům.

Identifikátory objektů ve značkách jsou unikátní hodnoty vzešlé z mezinárodních dohod, které přidělují národům unikátní čísla pro jednotlivé části bezpečnostních značek. Např. US

DoD (americké ministerstvo obrany) má identifikátor 1.3.6. Identifikátory objektů jsou užívány v mnoha protokolech a jsou velmi důležité pro bezpečnostní značkování dat. Následující text uvádí možnou reprezentaci bezpečnostní značky v jazyku XML:

```
<SecurityLabel>
        <securityPolicyId id="2.16.840.1.101.2.1.12.0.4"/>
        <securityClassification lacv="4"/>
        <privacyMark>SECRET</privacyMark>
        <securityCategory id="2.16.840.1.101.2.1.8.1">
        <missiSecurityCategories>
        <standardSecurityLabel>
        <namedTagSet id="2.16.840.1.101.2.1.12.0.4.3.1">
        <securityTag tagType="restrictive">
        <attributeFlags>
        <bit>5</bit>
        </attributeFlags>
        </securityTag>
        </namedTagSet>
        <namedTagSet id="2.16.840.1.101.2.1.12.0.4.3.10">
        <securityTag tagType="tagType7" tag7Encoding="bitSetAttributes">
        <attributes>
        <bit>17</bit>
        </attributes>
        </securityTag>
        </namedTagSet>
        </standardSecurityLabel>
        </missiSecurityCategories>
        </securityCategory>
 </SecurityLabel>
```

Popis jednotlivých částí bezpečnostní značky je dán odpovídajícími standardy a dále rozšiřován jejich dodatky pro specifický popis a možnost třídění informací v závisloti na jejich použití (varovné zprávy, výstupy vojenských systémů apod.).

3.2.7.3 Komponenty bezpečnostní značky

Bezpečnostní značka má tyto komponenty:

- Bezpečnostní Politika. Identifikátor objektu, který definuje politiku a je hodnotou přiřazenou organizací nastavující politiku. To dává možnost mít v bezpečnostní značce implementovánu více než jednu Bezpečnostní Politiku

- Klasifikace. Bezpečnostní klasifikace je reprezentována přirozeným 6-ti místným číslem, určujícím klasifikaci (unmarked; unclassified; restricted; confidental; secret; top secret). Sémantika dalších možných hodnot (korporátní stupně utajení) jsou popř. dále definovány v Bezpečnostní Politice a Klasifikace na ně poté odkazuje.
- Kategorie. Bezpečnostní značka může mít více než hodnotu Kategorie. Syntaxe a sémantika reprezentující kategorie může být odlišná v závislosti na Bezpečnostní Politice. Hodnota kategorie se skládá z identifikátoru objektu a dalších dat, jejichž syntaxe a sémantika je identifikátorem definována.
- Soukromá značka. Řetězec String, hodnota, která je zobrazena, nebo vytištěna spolu s bezpečnostní značkou („Můj dokument“ apod.).

Tato struktura zahrnuje všechny nezbytné informace a je zakódována do kompaktního souboru. Klíčovou vlastností je flexibilita značky, může být použita prakticky kdekoliv a zahrnout jakoukoliv Bezpečnostní Politiku.

Bezpečnostní značka je asociována s objektem, ke kterému je vytvořena. Např. pro dokument, nebo zprávu může být bezpečnostní značka implementována přímo do objektu.

3.2.8 Elektronická reprezentace bezpečnostního prověření uživatele

Bezpečnostní prověření uživatele je definován standardem X. 501 a má strukturu korespondující s bezpečnostní značkou.

Reprezentace bezpečnostního prověření uživatele v jazyku XML:

```
<Clearance>
	<securityPolicyId id="2.16.840.1.101.2.1.12.0.4"/>
	<securityClassification lacv="1"/>
	<securityClassification lacv="2"/>
	<securityClassification lacv="3"/>
	<securityCategory id="2.16.840.1.101.2.1.8.2">
	<SSLPrivileges>
	<namedTagSetPrivilege id="2.16.840.1.101.2.1.12.0.4.3.1">
	<securityTagPrivilege tagType="restrictive">
	<attributeFlags>
	<bit>5</bit>
	</attributeFlags>
	</securityTagPrivilege>
	</namedTagSetPrivilege>
	</SSLPrivileges>
	</securityCategory>
</Clearance>
```

3.2.8.1 Komponenty bezpečnostního prověření uživatele

Bezpečnostní prověření má tyto komponenty:

- Bezpečnostní Politika. Identifikátor objektu jako u bezpečnostní značky.
- Kategorie, stejné jako u bezpečnostní značky.
- Seznam prověření. Jedná se o seznam, reprezentovaný proměnnou bit string (sekvencí bitů), která koresponduje s integer reprezentací klasifikace bezpečnostních značek. Důvodem je občasná chybějící klasifikace informace k porovnání. Bezpečnostní prověření „nabídne“ ve svém těle všechny typy prověření svého uživatele a je možné informaci dodatečně prověřit v dalších krocích.

Struktura je velmi podobná proto není složité provádět jednoznačné porovnávání bezpečnostních značek a bezpečnostního prověření uživatele.

Bezpečnostní prověření je svázáno s uživatelem. Podobným přístupem může být vložení bezpečnostního prověření uživatele přímo k jeho uživatelskému účtu (Active Directory, LDAP apod.), pak je uživatel jasně identifikovatelný a není třeba dodatečného software pro svázání prověření s uživatelským účtem.

3.2.9 Elektronická reprezentace Bezpečnostní Politiky

Bezpečnostní Politika je velmi důležitá část mechanismu bezpečnostního značkování a bezpečnostního prověřování uživatele. Jejím použitím je možné použít jedinou reprezentaci objektu (jeho zabezpečení) v různých informačních systémech, různými Bezpečnostními Politikami. Uživatel, který má oprávnění francouzské vlády nebude mít (obvykle) přístup k dokumentům vlády britské. Politika bezpečnostní značky a bezpečnostního prověření uživatele musí souhlasit k přístupu k dokumentu a Bezpečnostní Politika je klíčovou částí jak toho dosáhnout – referenční porovnávací mechanismus.

Bezpečnostní Politika je rovněž důležitá pro definici, která úroveň klasifikace a jaká kategorie jsou ve značkách použity. Elektronická reprezentace Bezpečnostní Politiky musí zabezpečovat všechny tyto vlastnosti, musí podporovat bezproblémové sdílení i update informací a jejich atributů.

Jsou dva standardy, kterými se dá snadno elektronicky reprezentovat Bezpečnostní Politika. Je vytvářen tzv. SPIF (Security Policy Information File) na základě těchto standardů:

- X. 841, „Security techniques – Security information objects for access control“ vydaném ITU (Mezinárodní telekomunikační unií),
- SDN. 801, „Access control concept and mechanism“, publikovaném americkou NSA.

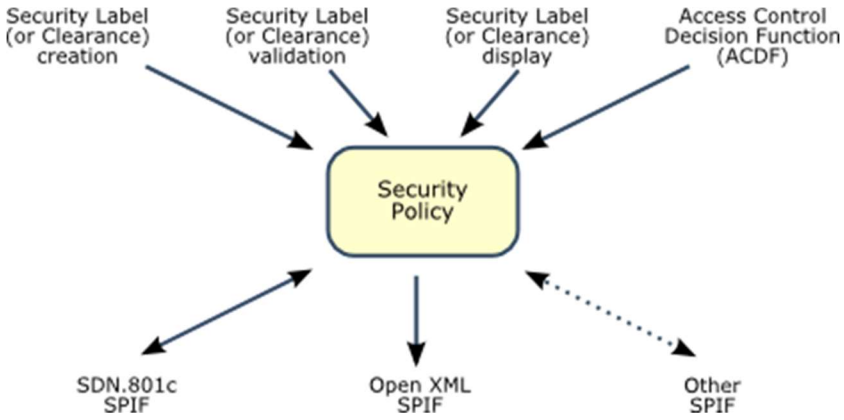
Tyto dva standardy mají velmi podobné schopnosti, ale nejsou kompatibilní. Benefitem používání standardizovaného řešení pro tvorbu SPIF je možnost jej pak libovolně šířit na různé systémy různých výrobců.

3.2.9.1 SPIF

Bezpečnostní politika (SPIF – Security Policy Information File) je v technickém pojetí XML soubor obsahující definici bezpečnostní politiky ke strojovému porovnávání. Bezpečnostní politika je vytvořena s ohledem na účel použití bezpečnostní domény, stupeň zabezpečení, požadavky na informační toky a požadavky klientů (uživatelů).

SPIF je XML schéma, poskytující volně dostupnou reprezentaci obecné bezpečnostní politiky, šablonu. XML dokumenty vytvořené podle tohoto schématu pak již popisují specifické bezpečnostní nastavení a za použití Stylesheets [10] mohou být konvertovány do velké škály jiných formátů, včetně textových formátů a i mnohem komplexnějších (např. standard SDN. 801 – sémantické rozšíření SPIF).

SPIF není vázán na jeden formát, podporuje více formátů a je snadné i komunikovat nebo zahrnout Bezpečnostní Politiky jiných systémů.



Obrázek 8 Architektura Bezpečnostní Politiky

Bezpečnostní Politika mohou být načtena nebo zapsána do SPIF souboru. To umožňuje použití alternativních SPIF formátů a jejich vzájemné konverzi. Dva nejznámější formáty SPIF jsou:

- Open XML SPIF
- SDN. 801c

Možná reprezentace Bezpečnostní Politiky v jazyku XML:

```
<?xml version="1.0" encoding="UTF-8"?>
< sp:SPIF xmlns:spif="http://www.xmlspif.org/spif"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.xmlspif.org/spif http://www.xml-
spif.org/schema/xmlspif.xsd"
    creationDate="2005021910000Z" rbacId="2.16.840.1.101.2.1.8.1"
    originatorDN="o=smhs ltd,c=gb" privilegeId="2.16.840.1.101.2.1.8.2"
    keyIdentifier="12345678">
    <spif:securityPolicyId id="1.2.3.4" name="Simple"/>
    <spif:securityClassifications>
        <spif:securityClassification name="Unclassified" lacv="1" hierarchy="1"/>
        <spif:securityClassification name="Restricted" lacv="2" hierarchy="2"/>
        <spif:securityClassification name="Confidential" lacv="3" hierarchy="3"/>
        <spif:securityClassification name="Secret" lacv="4" hierarchy="4"/>
        <spif:securityClassification name="Top Secret" lacv="5" hierarchy="5"/>
    <spif:securityClassifications>
< /spif:SPIF>
```

3.2.10 Kontrola bezpečnostní značky oproti bezpečnostnímu prověření uživatele

Základní kontrola bezpečnostní značky oproti bezpečnostnímu prověření uživatele je prováděna, když je bezpečnostní značka zpracována Hraničním Guardem a informaci je přidělena lokální interní bezpečnostní značka odpovídající formátu lokálního informačního systému (značka je „namapována“).

Reprezentace bezpečnostního prověření uživatele v jazyku XML:

```
<Clearance>
	<securityPolicyId id="2.16.840.1.101.2.1.12.0.4"/>
	<securityClassification lacv="1"/>
	<securityClassification lacv="2"/>
	<securityClassification lacv="3"/>
	<securityCategory id="2.16.840.1.101.2.1.8.2">
	<SSLPrivileges>
	<namedTagSetPrivilege id="2.16.840.1.101.2.1.12.0.4.3.1">
	<securityTagPrivilege tagType="restrictive">
	<attributeFlags>
	<bit>5</bit>
	</attributeFlags>
	</securityTagPrivilege>
	</namedTagSetPrivilege>
	</SSLPrivileges>
	</securityCategory>
</Clearance>
```

Uživatel se žádá o přístup k datům označených následující jednoduchou a neúplnou bezpečnostní značkou:

```
<SecurityLabel>
	<securityPolicyId id="2.16.840.1.101.2.1.12.0.4"/>
	<securityClassification lacv="4"/>
</SecurityLabel>
```

Kontrola bezpečnostní značky oproti bezpečnostnímu prověření uživatele bude v tomto případě neúspěšné. Uživatel nemá právo přístup k dokumentaci označené „Top Secret“ (tag SecurityClassification, hodnota = 4, uživatel vlastní prověření pouze 1, 2 a 3). Kontrolní mechanismy porovnávají bezpečnostní značky informací proti bezpečnostnímu prověření uživatele, to vše v kontextu Bezpečnostní Politiky.

3.2.11 Integrace bezpečnostní značky s digitálním podpisem

Bezpečnostní značky a bezpečnostní prověření uživatele jsou často používány organizacemi s přísnými všeobecnými bezpečnostními požadavky na ochranu dat. Je žádoucí tyto požadavky dále kombinovat s použitím digitálního podpisu.

Nejdůležitějším použitím digitálního podpisu v kontextu bezpečnostního značkování dat je jeho použití pro svázání bezpečnostní prověření uživatele s uživatelským účtem. Provádí se na základě standardu X. 509 pro nakládání digitálními certifikáty, který může obsahovat standard X. 501 pro bezpečnostní prověření uživatele – taková integrace pak naprosto jed-

noznačně identifikuje uživatele v informačním systému. X. 509 digitální certifikát může obsahovat více polí k popisu uživatele, např. emailovou adresu, digitální certifikát tak může být použit pro svázání bezpečnostního prověření uživatele i s jiným atributem (jménem) než systémovým jménem uživatele.

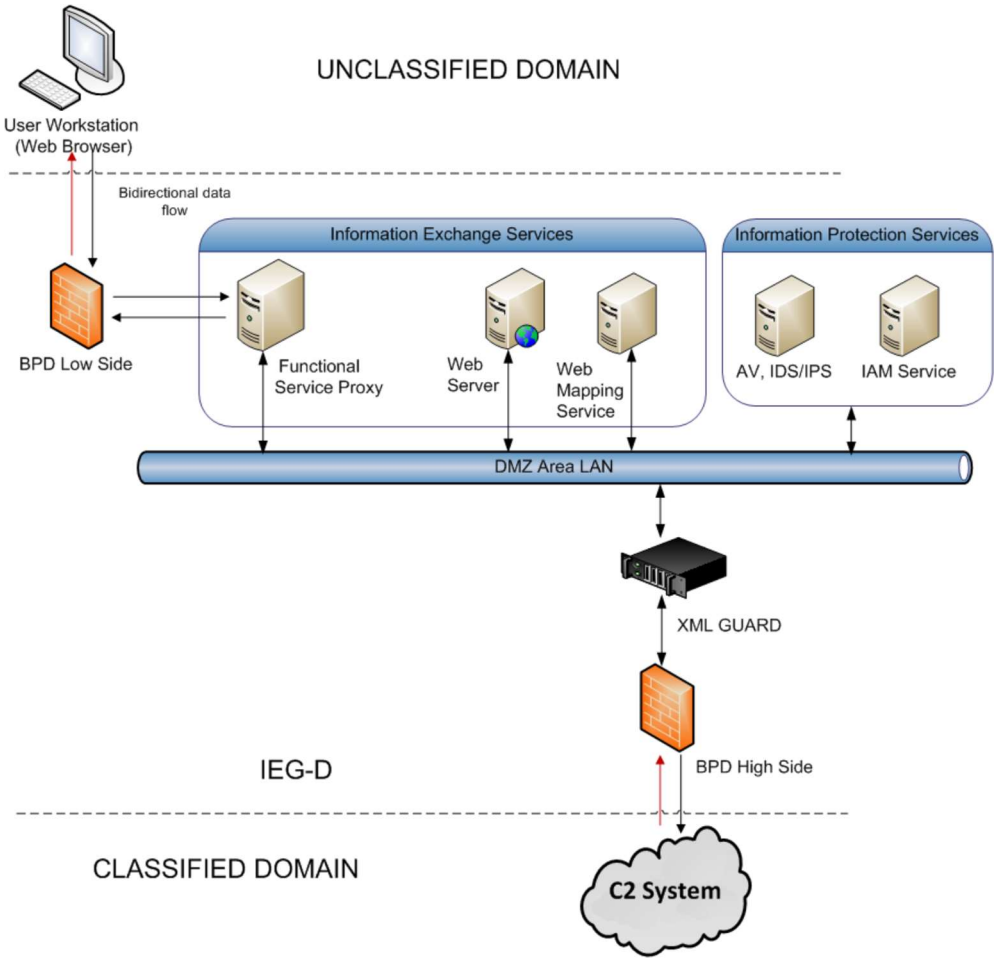
Bezpečnostní značka je asociována s každou informací, např. vložena do emailové zprávy. Jsou-li použity digitální certifikáty, je nutné aplikovat je jak na bezpečnostní značku, tak také na emailovou zprávu. Musí být ekvivalentní k vyloučení porušení poškození jak zprávy, tak značky. To znamená, že mechanismus digitálního podpisu musí být součástí standardu řešícího bezpečnostní značkování. Digitální podpis byl implementován postupně do standardů RFC 2634, STANAG 4406, X. 400 Messaging a X. 500 standardu pro adresářové struktury.

3.3 Technické aspekty mechanismu bezpečnostního značkování dat

Bezpečnostní značkování je založeno na standardu XML IETF RFC 2634 a obsahuje další přídavné části k umožnění požadavků na nakládání informacemi (práce s informací, zadržení, kontrola apod.). Aby bylo možné informací takto nakládat je pro tvorbu bezpečnostní značky použit jazyk XML (eXtemsible Markup Language). XML poskytuje otevřený a flexibilní mechanismus, který může být integrován do mnoha datových typů a snadno čitelný mnoha aplikacemi. Pro obecný popis značky je definováno XML schéma (STANAG 4774) a schéma je poté dále rozpracováno pro použití v jednotlivých specializovaných aplikacích, které mohou vyžadovat vlastní dodatečné prověření informace, nebo přídavné atributy, kterými budou informace tříděny (mapové podklady, polohové zprávy apod.).

3.3.1 Popis XML Guard

Architektura propojení bezpečnostních domén vyšší a nižší úrovně utajení je umožněna za použití brány IEG. Brána IEG obsahuje bezpečnostní komponenty, jedním z nich je XML Guard. Umístění prvku XML Guard naznačuje Obrázek 9. Propojení bezpečnostních domén na úrovni kontroly a správy bezpečnostních značek dat probíhá prostřednictvím XML Guard [11].

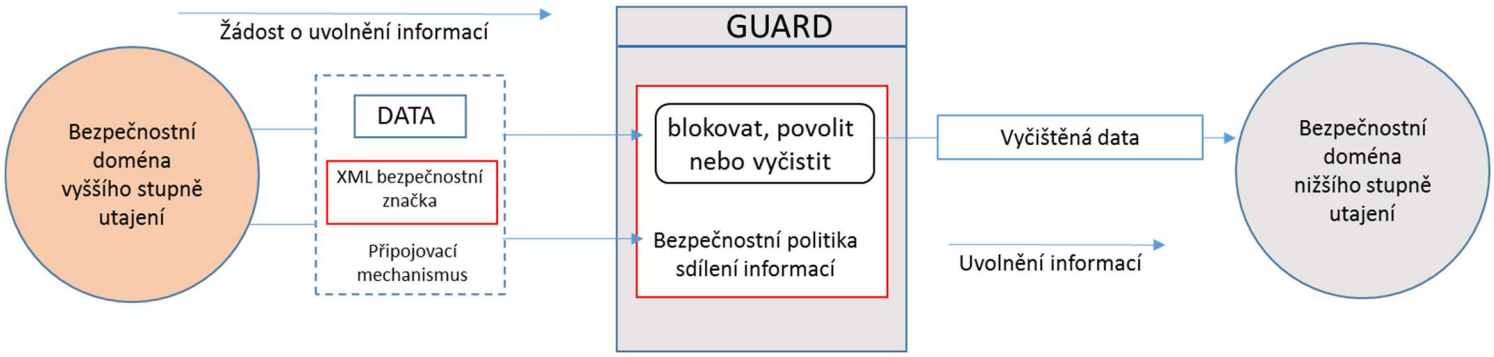


Obrázek 9 Umístění prvku XML Guard

Obrázek 10 Značkování informací a jejich filtrování

XML Guard zajišťuje kontrolu dat na základě platných bezpečnostních politik a zajišťuje jejich uplatňování na definovanou množinu příchozích dat. Funkce XML Guard je obousměrná, zajišťuje zamezení vstupu do bezpečnostní domény neautorizovaným uživatelům, nebo omezuje přístup do určitých oblastí informačního systému, ale rovněž kontroluje odchozí data informačního systému a zabraňuje neautorizovanému úniku dat.

Tento model závisí na dostupnosti mechanismu bezpečnostního značkování informací v bezpečnostní doméně vyššího stupně utajení. Model podporuje jak značkování jednotlivých atributů a částí informace, tak značkování celé informaci (většina případů). XML Guard je nakonfigurován za použití bezpečnostním politik, aby podával rozhodnutí, zda informace smí, nebo nesmí být uvolněna do jiné bezpečnostní domény. Bezpečnostní politika musí být aplikována tvůrcem informace na každou jednotlivou informaci (nebo tvořenou skupinu) informací zvlášť. Informace je poté strukturovaný set dat, ke kterému je připojena bezpečnostní značka.

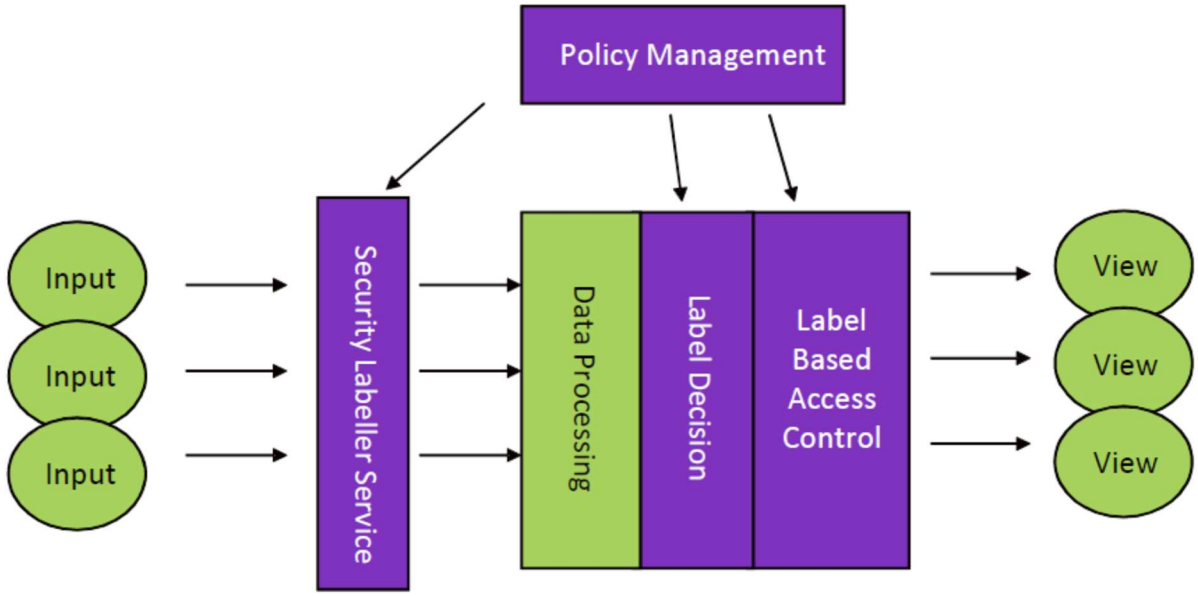


Obrázek 11 Provádění čištění informací

Bezpečnostní mechanismus značkování dat dle definice NATO může dle nastavení provádět inspekci každého jednotlivého elementu informace, který je opatřen bezpečnostní značkou. Výsledkem je možnost uvolnění informace „vyčištěné“. Nejsou-li splněna kritéria pro uvolnění informace, nemusí být její uvolnění zamítnuto úplně, ale uvolněny pouze odpovídající části. Ty neodpovídající budou odstraněny, nebo jejich obsah nahrazen (většinou textem spravujícím čtenáře o nutnosti utajení a nedostupnosti textu) viz Obrázek 11.

3.3.2 Popis značkovacího mechanismu

Základním krokem k zabezpečení systému je implementace mechanismu bezpečnostního značkování a jeho standardů (confidentialy labelling a binding). Značkování probíhá dle logického schématu na Obrázek 12 (řešení firmy Nexor používané v NATO) [5].



Obrázek 12 Logická struktura značkování dat

Popis služeb značkovacího mechanismu:

- Policy Management

Správa Bezpečnostní Politiky

- Security Labeller Service

Vstupní data jsou z více zdrojů, např. se jedná o dokumenty na úložišti, přílohy emailů, streamovaná data. Pro zajištění konzistentního zpracování z hlediska bezpečnosti informací, je nutné každé informaci přiřadit bezpečnostní značku. V řešení je použita služba Security Labeller Service na bázi SOAP protokolu, která zajišťuje:

  - Zjištění existence bezpečnostní značky
  - Pokud značka není přiřazena, pak přiřazení defaultní značky,
  - Pokud značka existuje, zkontrolovat dokument je-li značka adekvátní povaze dokumentu.

Jsou použity technologie např. MS Office Word header a SOAP/XML Envelope.

- Data Processing

Služba Data Processing provádí kontrolu operací nad daty a zajišťuje konzistenci bezpečnostní značky (monitoruje a zabraňuje možnému poškození, změny a zničení značky aplikacemi), např.: funkce fúze dat, sdílení informací na webovém portálu, nebo společná práce více uživatelů na jednom dokumentu.

- Label Decision

Pokud chce uživatel přistoupit k informacím, je požadováno systémové rozhodnutí (schválení/neschválení) dle bezpečnostní značky. Pro přístup k jednomu dokumentu je situace poměrně jednoduchá, je kontrolována jediná značka. Pro společnou práci na dokumentu, nebo přístupu současně k více dokumentům naráz je již potřeba komplexnější rozhodnut. Je použito služby na základě protokolu SOAP, která zpracuje žádost, vyhodnotí individuální nebo společné přístupy k datům a podá zhodnocení.

- Label-Based Access Control

V tomto stádiu již bezpečnostní mechanismus identifikoval informace, které žadatel o zpřístupnění žádá, byl zhodnocen jeho přístup a oprávnění. Kontrolní mechanismy povolily nebo zamítly přístup k datům. Access Control služba je poskytována Guardem a je složena z následujících komponent:

  - XML
  - Directory
  - Filestore
  - Web services

Služba zpracovává XML schéma politiky, v úložišti je připravenu informaci. Čte XML připojený soubor informace, porovnává údaje s bezpečnostní politikou. Ověřuje identitu uživatele v adresářové službě – poskytuje přístup [12].

3.3.3 SOAP protokol

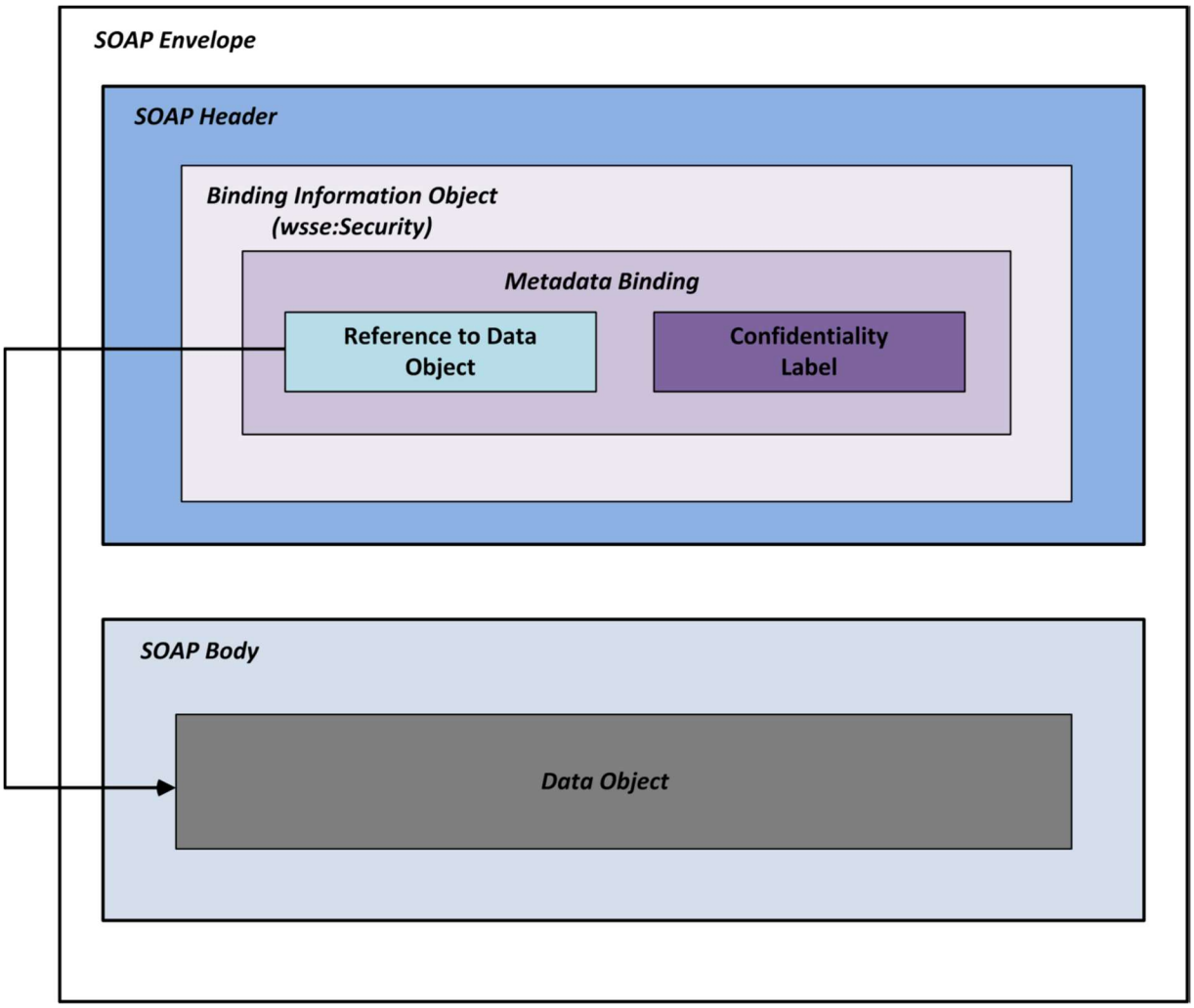
Základním přenosovým protokolem mechanismu bezpečnostního značkování dat je SOAP protokol pro zabezpečení posílání zpráv XML a je základem webových služeb. Ostatní standardy jako WSDL a UDDI vznikly až později po uvedení SOAPu a jen dále rozšiřují jeho možnosti a snadnost použití. SOAP umožňuje zaslání XML zprávy mezi dvěma aplikacemi a pracuje tedy na principu peer-to-peer. Zpráva je jednosměrný přenos informace od odesílatele k příjemci, ale díky kombinování několika zpráv můžeme pomocí SOAPu snadno implementovat běžné komunikační scénáře.

Nejčastěji se SOAP používá jako náhrada vzdáleného volání procedur (RPC), tedy v modelu požadavek/odpověď. Jedna aplikace pošle v XML zprávě požadavek druhé aplikaci, tak požadavek obslouží a výsledek zašle jako druhou zprávu zpět původnímu iniciátorovi komunikace. V tomto případě bývá webová služba vyvolána webovým serverem, který čeká na požadavky klientů a v okamžiku, kdy přes HTTP přijde soapová zpráva, spustí webovou službu a předá jí požadavek. Výsledek služby je pak předán zpět klientovi jako odpověď.

3.3.3.1 Struktura zprávy XML v SOAP protokolu

Zpráva v SOAPu je jednoduchý XML dokument, který má kořenový element Envelope. V této obálce jsou pak uzavřeny dva elementy Header (hlavička) a Body (tělo). Hlavička je v obecné SOAP obálce nepovinná a používá se pro přenos pomocných informací pro zpracování zprávy – například identifikaci uživatele, autentizační informace (jméno, heslo) apod. Při použití tohoto protokolu pro přenos bezpečnostních značek informací je však nepostradatelná. Obsahuje výše jmenované základní informace o zabezpečení dat, které jsou nezbytné pro účel značkování dat. Hlavička zprávy je kontrolována bezpečnostními mechanismy a dle výsledků kontroly je určeno, jak bude informací nakládáno.

Dále následuje tělo zprávy, v němž se přenášejí informace identifikující volanou službu a předávané parametry, resp. návratové hodnoty služby. SOAP používá jmenné prostory pro identifikování jednotlivých částí XML zprávy.



Obrázek 13 SOAP Envelope

Jelikož se dnes SOAP typicky používá pro RPC volání, je celkem přirozené, že se pro přenos požadavku/odpovědi nejčastěji používá protokol HTTP (HyperText Transfer Protocol). Důvodem je zejména široká podpora HTTP v různých aplikacích. Navíc webovou službu lze

nahrát přímo na běžný webový server, jenž slouží jako „dispečer“, který jednotlivé požadavky předává odpovídající webové službě ke zpracování. Výhoda použití HTTP také spočívá v tom, že stávající síťová infrastruktura, dovoluje v podstatě neomezenou komunikaci na portu vyhrazeném pro HTTP (TCP port 80). Webové služby je možné používat bez nutnosti zásahu do konfigurace aktivních síťových prvků, jako jsou firewally. Při použití technologií DCOM nebo CORBA je potřeba povolit komunikaci na portech, které používají příslušné přenosové protokoly (např. IIOP pro CORBA).

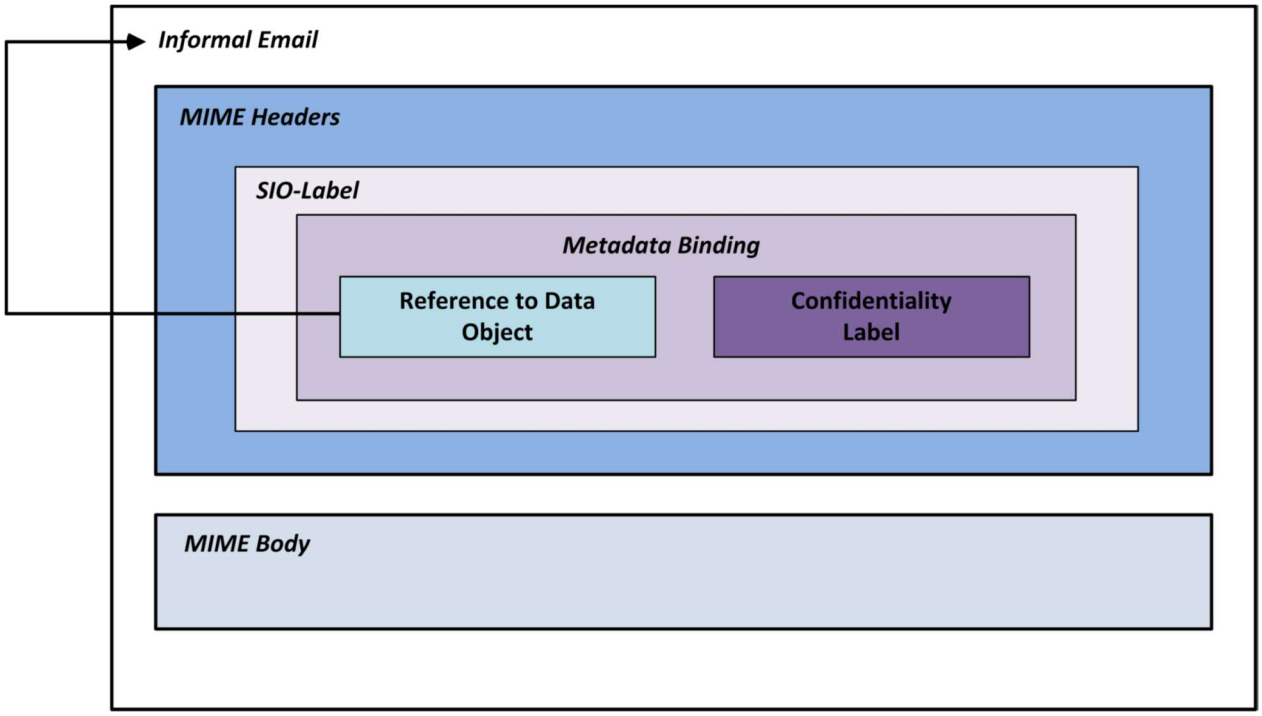
SOAP požadavek se zasílá v těle HTTP požadavku. Používá se přitom metoda POST, která dovoluje posílat data v těle HTTP požadavku. Požadavek musí obsahovat HTTP hlavičku SOAPAction, která identifikuje SOAP požadavek. Tuto hlavičku mohou používat jednak firewally k filtrování požadavků a jednak může obsahovat URI s identifikací služby, která se má vyvolat.

Jednotlivé implementace webových služeb podporují i další přenosové mechanismy. Patří mezi ně například přenos pomocí e-mailových zpráv pomocí protokolu SMTP (Simple Mail Transfer Protocol) nebo XMPP (Extensible Messaging and Presence Protocol) [13].

3.3.4 SMTP protokol

Simple Mail Transfer Protocol je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP. Jedná se o jednu z nejstarších aplikací, původní norma RFC 821 byla vydána v roce 1982 (v roce 2001 ji nahradila novější RFC 2821). SMTP funguje nad protokolem TCP, používá port TCP/25 pro komunikaci mezi poštovními servery a port TCP/587 pro příjem e-mailů od e-mailových klientů [14].

Ve své hlavičce obsahuje SMTP protokol bezpečnostní značku zasílaného objektu, který je posléze kontrolován.



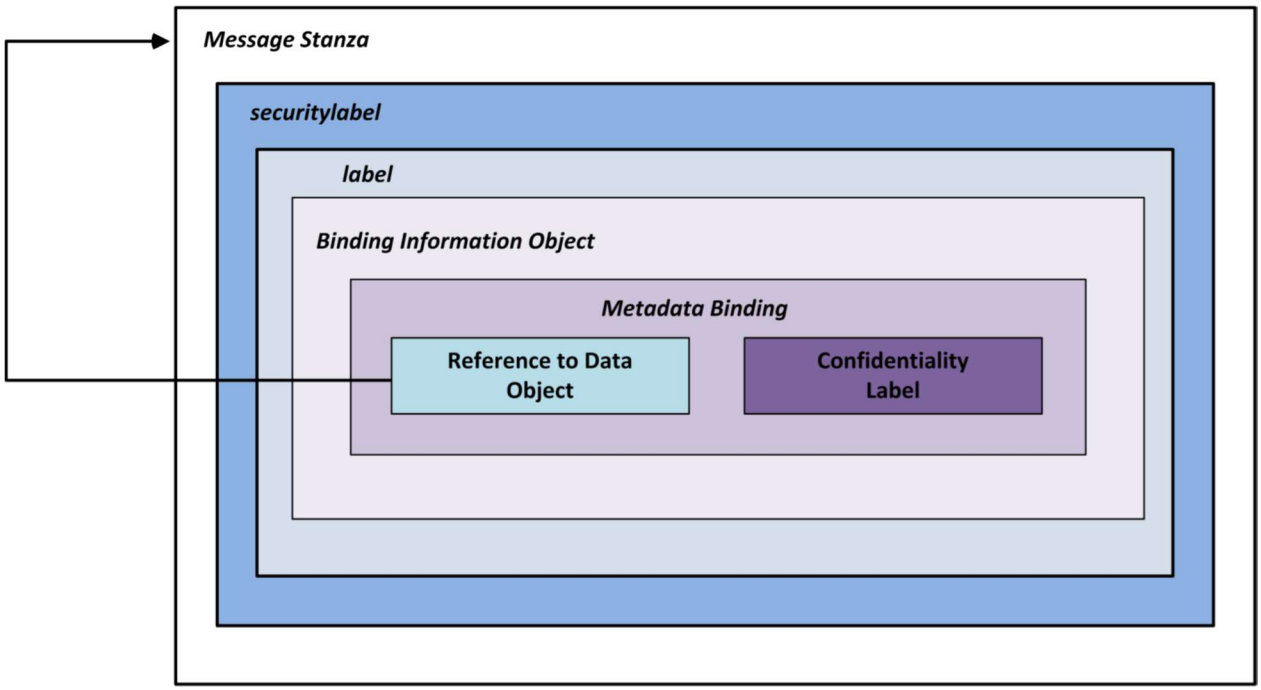
Obrázek 14 Bezpečnostní značka zprávy protokolu SMTP

3.3.5 XMPP protokol

Extensible Messaging and Presence Protocol (XMPP) vznikl jako protokol pro komunikaci v reálném čase dvou a více klientů počítačové sítě Jabber. Od počátku je protokol vystavěn pro jednoduchou rozšiřitelnost, a tak jej lze snadno využít i pro vzájemnou komunikaci heterogenních systémů a ovládání automatizovaných služeb. Komunikace mezi uživateli probíhá tak, že je nejprve kontaktován doménový server odesílajícího uživatele a ten odešle zprávu na cílový doménový server příjemce zprávy, který jej doručí konkrétnímu klientovi. Nejedná se tedy o přímou, ale o zprostředkovanou komunikaci mezi aktéry. V roce 2004 byl protokol XMPP publikován jako RFC standard RFC 3920: Extensible Messaging and Presence Protocol (XMPP). XMPP protokol přenáší XML elementy za účelem výměny zpráv a informací v reálném čase. Mezi základní elementy popsané v RFC 3920 patří tagy:

- <message/>,
- <presence/>,
- <iq/> ,

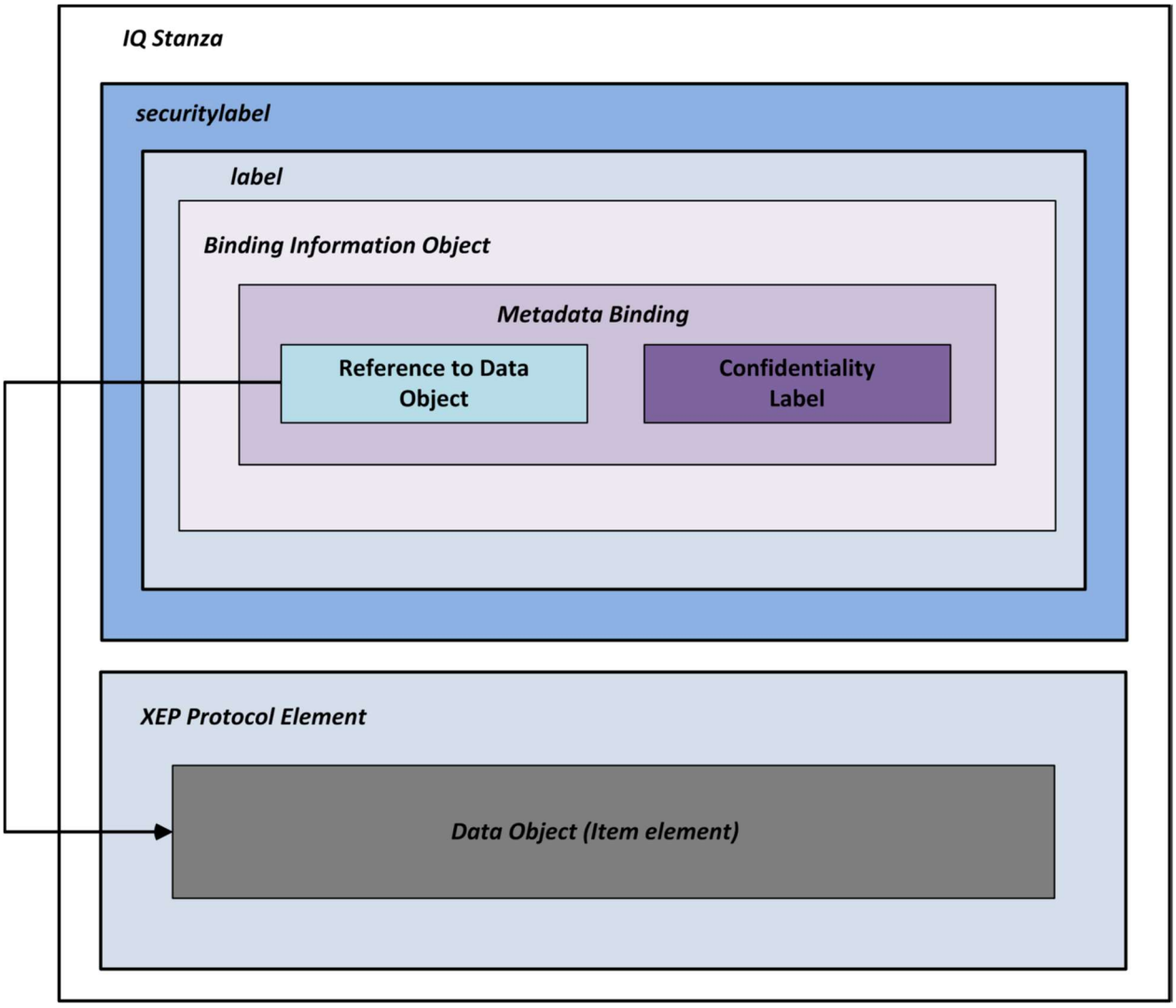
umožňující přenos aplikačně specifických dat. Pomocí XEP (XMPP Excension Protocols) je dále možné rozšiřovat množinu základních vlastností definovaných ve výše uvedených RFC [15].



Obrázek 15 Bezpečnostní značka v tagu Message

Na Obrázek 15 je zobrazena stať zprávy (Stanza) posílané protokolem XMPP s bezpečnostní značkou informace dle rozšíření XEP-0258: Security Labels in XMPP v části Message.

Na Obrázek 16 je zobrazena stať zprávy (Stanza) posílané protokolem XMPP s bezpečnostní značkou informace dle rozšíření XEP-0258: Security Labels in XMPP v části IQ [16].



Obrázek 16 Bezpečnostní značka v tagu IQ

3.4 Dílčí závěr

Bezpečnostní značky a bezpečnostní prověření uživatele jsou důležitou součástí kontrolního mechanismu přístupu k informacím. Mohou být provedeny elektronicky ve formátech umožňující jejich použití v široké škále různých platforem a softwarových řešení a dodatečným zabezpečením může být použití digitálního podpisu.

II. PRAKTICKÁ ČÁST

4 IMPLEMENTACE MECHANISMU ZNAČKOVÁNÍ DAT DO STÁVAJÍCÍHO INFORMAČNÍHO SYSTÉMU

Nejrychlejším implementací řešení bezpečnostního mechanismu značkování je implementace značkovacího serveru se všemi komponenty. Ten bude působit jako interface pro více připojených bezpečnostních domén (entit) a bude překládat (povolovat) bezpečnostní značky informací všech domén. Také bude provádět připojování bezpečnostních značek k vytvářeným datům. Tento server bude pouze vložen do stávajícího informačního systému.

Následným krokem vývoje bude implementace značkovacího serveru do každé bezpečnostní domény a správa bezpečnostní politiky jak společné, tak i možnost vytvoření vlastní podřízené. Zde musí zajištěno, že servery budou dále rozvíjeny v souladu s požadavky na zabezpečovací mechanismus, tj. všechny servery v bezpečnostních doménách budou stejné úrovně, budou poskytovat stejné služby se stejnými standardy, bude vytvořeno společné prostředí pro sdílení informací. Další rozvoj bezpečnostního značkování (pro další typy dat, další typy bezpečnostních domén atp.) musí být implementován do všech serverů ve všech bezpečnostních doménách.

Nejpokrokovějším řešením je implementace značkovacího serveru (služby, aplikace) na straně klienta. Jedná se o sloučení funkcionality bezpečnostního značkování s uživatelským prostředím. Každý klient (uživatel) je poté sám o sobě důvěryhodný systém s integrovanou bezpečnostní politikou založenou na všeobecných standardech, tedy přenositelnou z prostředí do prostředí.

4.1 Fáze implementace

Implementace mechanismu značkování dat do stávajícího informačního systému probíhá ve čtyřech fázích. Pro každou fázi musí být splněny dílčí kroky, každý dílčí krok zvyšuje celkovou úroveň zabezpečení původního systému.

Koncept popisuje 4 evoluční fáze vývoje podobného systému.

4.1.1 1. fáze

1. Popis
    - Formát značkování dat a tvorba připojovacích souborů je specificky vytvořena pro jednu oblast produkce dat (jednu aplikaci, jednu sadu aplikací, databázi apod.).
    - Značky a připojovací soubory neumožňují ve většině případu zautomatizované zpracování verifikací a validací na základě bezpečnostní politiky. Rozhodnutí je často nutné provádět ručně.

- Použití metadat v připojovacích souborech není (nemusí být) standardizováno a v souladu s ostatními použitými typy metadat v systému. Nejsou použity vícenásobné hodnoty v bezpečnostních značkách, je možné občasné křížení a nesoulad bezpečnostních politik.
- Mechanismus bezpečnostního značkování je umístěn v systému vedle dalších nedůvěryhodných služeb, je možné jeho napadení, nebo systémové ohrožení neprověřenými procesy jiných aplikací využívající stejné systémové prostředky.
- Není implementován žádný kontrolní mechanismus zabezpečující kontrolu změny, nebo odstranění bezpečnostní značky.
- Sémantika použitá v připojovacím souboru je použitelná pouze v aplikaci, ve které byla vytvořena.
- Připojovací mechanismus neumožňuje připojení bezpečnostní značky pouze k částem dat/informací (pouze k určitým odstavcům dokumentu, tabulkám atd.) není umožněno částečné zabezpečení.

2. Kroky vedoucí ke zvýšení úrovně zabezpečení:
   - Přijmout standardy bezpečnostního značení a tvorby připojovací souborů,
   - Výstavba a implementace značkovacího serveru,
   - Značkovací server jednoznačně ověří identitu klienta (uživatele) dostupnými mechanismy na fyzické nebo logické vrstvě systému (např. ověření network interface, zdrojové IP adresy, účtem v Active Directory atp.).
   - Značkovací server musí být zprostředkovatelem požadavků na odeslání a přijetí informací mezi bezpečnostními doménami.

   Na konci fáze je v bezpečnostní doméně k dispozici značkovací server schopný generovat bezpečnostní značky pro datové soubory zvolených aplikací. Může existovat i více značkovacích serverů, není zabezpečen souběh vytváření více značek pro jediný soubor. V rámci značkovacího serveru je implementován Guard umožňující odesílání a přijímání dat.

4.1.2 2. fáze

1. Popis
   - Značkovací server zabezpečuje zjišťování identity klienta (uživatele), který je tvůrcem informace a požaduje pro ni bezpečnostní značku. Server je schopen vygenerovat značku automaticky, zatímco ve fázi 1 je vyžadována součinnost klienta (uživatele).
   - Ověření identity klienta (uživatele) a značkovacího serveru probíhá vzájemně.

- Jsou implementovány silné mechanismy autentizace uživatele založené na certifikátech.
- Klient (uživatel) a značkovací server ověřují integritu bezpečnostní politiky, která je použita, a to ověření její pravosti (politika musí být podepsána a zcertifikována z úrovně domain management autority.
- Prvek Guard a prvek značkovací server jsou nyní dvě oddělené entity.

2. Kroky vedoucí ke zvýšení úrovně zabezpečení:

   - Autentizace je prováděna na základě certifikátů PKI,
   - Jako přídavek k jednoznačné autentizaci uživatele v systému je rovněž s daty svázán certifikát tvůrce dat (digitální podpis dat),
   - Je implementován silný mechanismus připojování souborů metadat založený na PKI certifikátech,
   - Značkovací server má implementovány mechanismy pro verifikaci, které:
     - Umožňují provádět kontrolu bezpečnostní značek na základě bezpečnostních politik,
     - Verifikují formáty datových objektů dle vzorů pro daný typ informace,
     - Provádějí inspekci datových souborů na závadný obsah před provedením připojení,
     - Detekují možné úpravy a odstranění metadat připojených k informaci.

   Fáze 2 předpokládá úplnou implementaci infrastruktury PKI v informačním systému. Na konci druhé fáze je značkovací server schopen verifikovat datové objekty a porovnávat jejich bezpečnostní značky s uloženou bezpečnostní politikou. Zabezpečení informačního systému je zvýšeno použitím certifikátů infrastruktury PKI. Značkování dat probíhá automaticky bez vědomí uživatele.

4.1.3 3. fáze

1. Popis

   Zvýšení úrovně zabezpečení probíhá vývojem a rozvojem tzv. spirálovým přístupem. Tento přístup je nejdříve aplikován na implementované zabezpečovací mechanismy, tedy značkovací server:

   - Zvýšení úrovně zabezpečení značkovacího serveru je prováděno implementací dodatečných zabezpečovacích mechanismů, např. monitoring značkovacího procesu, sebeochranné mechanismy značkování apod.
   - Zvýšení úrovně zabezpečení použitého operačního systému, což zároveň zvyšuje úroveň zabezpečení značkovacího mechanismu na něm provozovaného.

- Zvýšení úrovně zabezpečení použitého hardware a to zejména použití šifrovacího zařízení umožňujícího bezpečnou komunikaci na nezabezpečené části přenosové trasy (internet, rádiové spojení, Wifi apod.).
- Opakování spirálového vývoje dokud není dosažena požadovaná úroveň zabezpečení.

Úroveň zabezpečení je dále rozvíjena spirálovým vývojem a je určena ke zvýšení schopností značkovacího serveru (řešení pro bezpečnostní značkování dat). Běžně jsou tato řešení provozována na víceúčelových operačních systémech (OS není určen pouze pro podporu tohoto řešení, ale je zde provozováno více typů aplikací), tímto přístupem se snažíme toto řešení co nejvíce zabezpečit.

2. Kroky vedoucí ke zvýšení úrovně zabezpečení:
   - Při použití kryptografického materiálu zabezpečení schválení národní bezpečnostní autority,
   - Použití adekvátního stupně zabezpečení a typu šifrovacího algoritmu pro provoz digitální podpisu informací,
   - Splnění bezpečnostních požadavků pro implementaci důvěryhodných softwarových řešení,
   - Implementace adekvátního hardware pro použití infrastruktury PKI (smart karty, klíče, certifikační autorita atd.).

Na konci fáze 3 bude značkovací server odpovídat požadavkům na úroveň zabezpečení informačního systému a dále rozvíjen iteracemi spirálového vývoje. Standardy pro značkování a tvorbu připojovacích souborů jsou dodržovány a je použita infrastruktura PKI.

4.1.4 4. fáze

- Systém používá PKI a kryptografické prostředky
- Systém je dále rozvíjen spirálovým vývojem
- Značkovací mechanismus je implementován na úroveň klienta (uživatele). Jsou použity obecné standardy. Značkovací mechanismus ve formě serveru je v celém systému nahrazen aplikací (službou) umožňující uživateli značkovat (zpracovat bezpečnostní požadavky na informaci) přímo ze svého uživatelského prostředí.
- Funkcionalita bezpečnostního značkování dat je jako proces prováděna okamžitě při vytvoření dat.

Fázi 4 si můžeme představit jako úplné splynutí značkovacího serveru s uživatelským prostředím. Výsledkem fáze 4 bude uživatelský vysoce zabezpečený informační systém s integrovanou standardizovanou schopností provádět bezpečnostní

značkování dat. Problémem ve fázi bude oddělení zabezpečeného procesu značkování dat, nyní provozovaném na bezpečném serveru (HW, OS, značkovací mechanismus), od standardního uživatelského víceúčelového prostředí. Jsou dva způsoby jak tento problém vyřešit:

1. Architektura uživatelského prostředí (systému) je nahrazena architekturou řešení pro provádění značkování realizované ve fázi 3. Uživatelské aplikace jsou upraveny pro provoz v tomto systému a musí splňovat požadavky na úroveň zabezpečení dosaženou ve fázi 3. Výsledkem je vysoce zabezpečený systém, ve kterém všechny aplikace, OS a použitý hardware splňují veškeré bezpečnostní požadavky. V mezidobí úprav aplikací pro soulad s architekturou značkovacího řešení je nutné implementovat monitorovací a kontrolní mechanismy pro kontrolu zatím neupravených aplikací.
2. Pokud použité aplikace uživatelského prostředí nemohou být upraveny, aby splňovaly výše uvedené kritéria, pak je architektura informačního systému upravena tak, aby pouze značkovací řešení (jako služba či aplikace) byl provozováno v zabezpečeném prostředí. Základem pro takové řešení je použití virtualizace, kdy výsledek fáze 3 je provozován v zabezpečeném prostředí virtualizačního hypervisoru.

Určitě je vhodné doporučit druhé řešení. Není nutné složitě upravovat COTS (Commercial-of-the-shelf) aplikace a popř. rovněž jednat s jejich výrobci o možných úpravách, ale také je toto řešení flexibilní pro jakoukoliv platformu a síťové prostředí.

Musí však být dodrženy a implementovány standardy pro provádění značkování dat a také jejich propojování s informacemi a rovněž jejich aktuální podoba (provádění aktualizací bezpečnostních politik). Také musí být zaručena včasná a vhodná úprava těchto mechanismů v závislosti na aktualizacích a úpravách těchto aplikací (nový update MS Office apod.). Dále musí být rovněž periodicky testována síla šifrovacího mechanismu určeného pro zajištění bezpečnosti připojení bezpečnostní značky k vyprodukované informaci z hlediska napadnutelnosti mechanismu a možnému pozměnění informace.

Na konci fáze 4 má každý klient (uživatel) k dispozici řešení provádějící bezpečnostní značkování, zajišťující zabezpečení každé vyprodukované informace bez ohledu na umístění v systému nebo použitý typ dat. Použitím standardizovaných řešení bezpečnostního značkování dat a mechanismu připojování souborů metadat, může nyní každý kontrolní bod (Guard) ve všech bezpečnostních doménách zpracovat jakýkoliv soubor a okamžitě jej porovnat s bezpečnostní politikou bez ohledu na použité komponenty.

4.2 Provedení

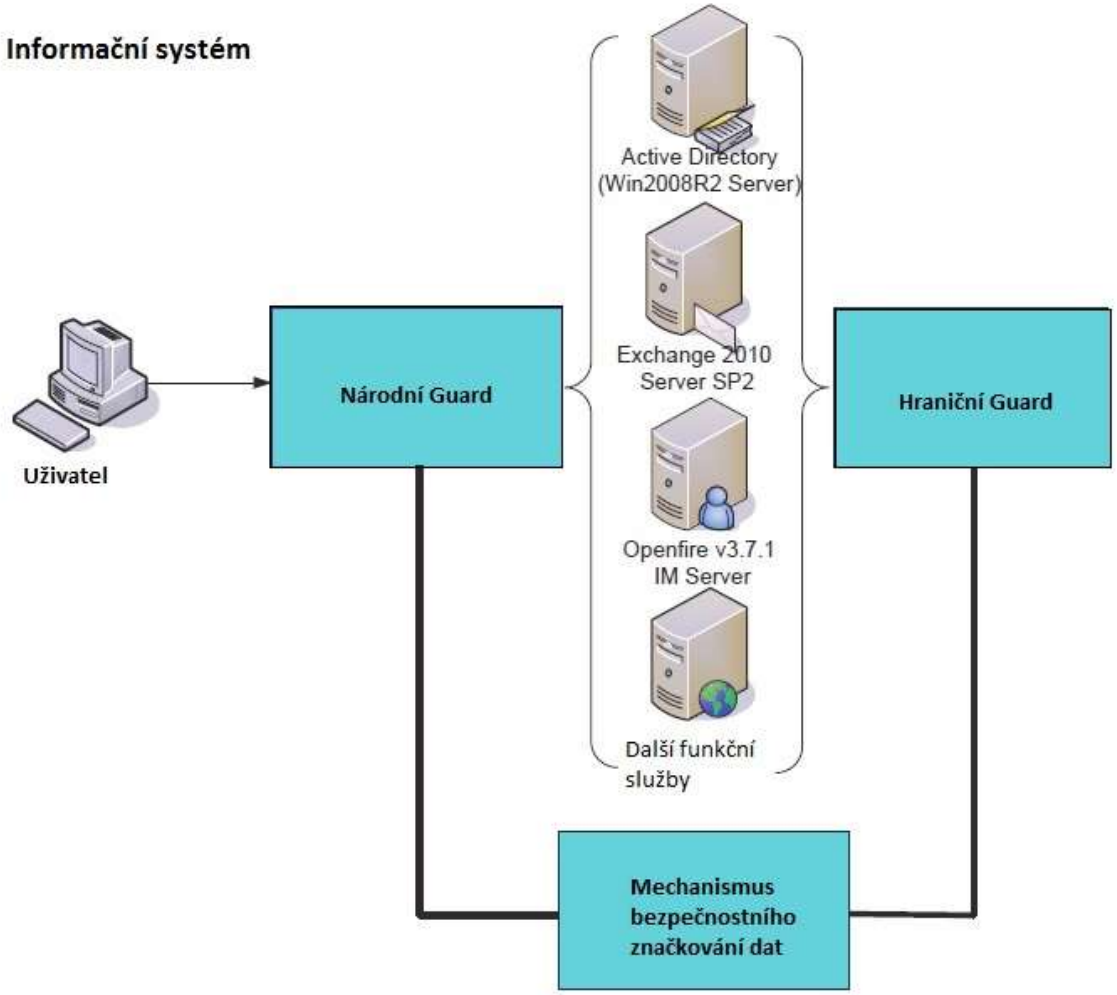
Implementace do stávajícího informačního systému je provedena pouze pro první fázi dle konceptu výstavby podobného řešení.

Implementace byla provedena do informačního systému obsahujícího doménový řadič, server pro zabezpečení služby Email a server pro zabezpečení služby Chat. Řešení bezpečnostního značkování dat je vloženo do původního informačního systému. Ten sestával z uživatelských stanic, serverového řešení pro služby Email a Chat a doménového kontroleru s implementovanou službou Active Directory. Do fiktivního informačního systému byly vloženy komponenty mechanismu bezpečnostního značkování dat.

4.2.1 Informační systém obsahuje tyto komponenty:

1. Servery
    - Doménový kontroler - OS Windows 2008 R2, služba Active Directory, DNS, DHCP, NTP
    - Emailový server - MS Exchange 2010 Standard
    - Server služby chat - OpenFire 3.7.1
    - Další možné funkční služby
2. Uživatelská stanice
    - Windows 7
    - MS Office 2010 (MS Oulook)
    - Spark – klient chatu

Lokální informační systém je vybaven vlastní národní lokální politikou pro zpracovávání dat a informací uvnitř systému a dále Bezpečnostní Politikou, která je známá i dalším partnerům a nastavena pro dodržování nakládání daty národního systému mimo jeho hranice. Na Obrázek 17 Implementace mechanismu bezpečnostního značkování do informačního systémuje zobrazena implementace mechanismu bezpečnostního značkování do informačního systému. Do informačního systému jsou vloženy Guardy, které provádějí inspekci komunikace klient-server a také server-server a zároveň posílají dotazy a požadavky Mechanismu značkování dat k určení odpovídajícího procesu jak naložit příchozí/odchozí informací. Národní

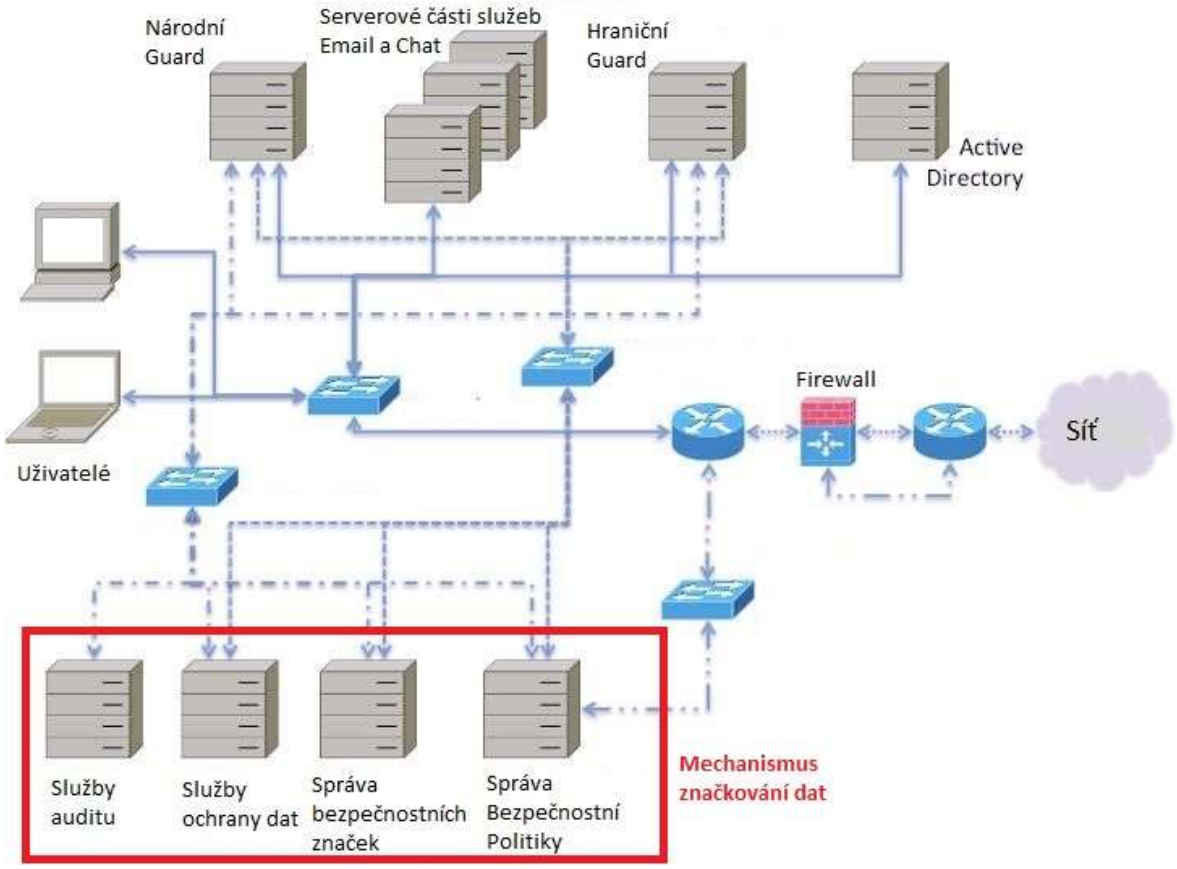


Obrázek 17 Implementace mechanismu bezpečnostního značkování do informačního systému

Guard je vložen mezi uživatelské stanice a serverová řešení a zajišťuje vynucování odpovídající Bezpečnostní Politiky. Když jsou data posílána od uživatele na server, Národní Guard aplikuje národní ochranu (lokální politiku a značkování), když uživatel požaduje data ze serveru, pak Národní Guard zkontroluje oprávnění, odstraňuje národní ochranu dat (lokální politiku a značkování) a zasílá je uživateli.

Pokud uživatel posílá nebo požaduje data ze serverů cizího systému, vstupuje do hry Hraniční Guard. Hraniční Guard provádí inspekci odpovídající Bezpečnostní Politiky u komunikace národ-národ. Pokud je tato komunikace požadována, pak konvertuje národní lokální politiku do Bezpečnostní Politiky, kontaktuje svůj protějšek – Hraniční Guard cizího informačního systému a předává data a informace. Hraniční Guard cizího systému poté postupuje analogicky.

Guardy i bezpečnostní mechanismus jsou kompletní aplikace (servery) dodávané buď komerční cestou (dodavatelé Nexor, ISODE, DeepSecure a další), nebo je možná implementace vlastního vyvinutého řešení. V tomto případě je uvažována implementace řešení firmy Bell Canada vyvíjející podobné řešení pro nasazení v kanadské armádě a dále ve státní



Obrázek 18 Detailní zapojení jednotlivých komponent mechanismu bezpečnostního značkování dat

správě. Guard je popisován jako blackbox plnící danou funkci, nasazený do informačního systému. Funkce Guardu jsou vysvětleny v kapitole 3.3.1. V reálném provedení budou (mohou být) všechny tyto komponenty implementovány do ochranného prvku IEG jako součást bezpečnostních mechanismů, které tento prvek poskytuje. Servery jsou poté provozovány za použití hypervisorů na virtualizační platformě.

4.2.2 Systémová konfigurace jednotlivých částí informačního systému

V ideálním případě je vhodné, aby jednotlivé části (servery) informačního systému byly instalovány ve virtuálním prostředí k dalšímu dodatečnému zabezpečení. Vedle standardních bezpečnostních komponent informačního systému jako jsou zabezpečený router (hardened), zabezpečené switche, firewall, antivirus atp. bude informační systém obsahovat:

4.2.2.1 Email

Emailový server musí být nakonfigurován:

- K příjmu SMTP a POP3 požadavků Národního Guardu,
- K zajištění směrování odchozí pošty (out-bound) na Hraniční Gaurd,

- K zajištění příjmu příchozí pošty cizích systémů (in-bound) předanou z Hraničního Guardu,
- Vyřizování vnitřní komunikace služby pošta za použití Národního Guardu.

Národní Guard musí být nakonfigurován:

- K příjmu POP3 a SMTP požadavků od připojených uživatelů,
- K příjmu požadavků SMTP z emailového serveru,
- K zajištění konektivity k Mechanismu bezpečnostního značkování.

Hraniční Guard musí být nakonfigurován:

- K příjmu SMTP požadavků emailového serveru,
- K příjmu server-to-server komunikace cizích systémů,
- Pro schopnost generovat tyto požadavky,
- K zajištění konektivity k Mechanismu bezpečnostního značkování.

Hraniční Guard provádí konverzi národní lokální politiky na Bezpečnostní Politiku.

Uživatelé mají ve svých poštovních klientech MS Outlook implementován dodatečný software Titus, zabezpečující funkcionalitu značkování emailové komunikace.

Veškeré POP3 a SMTP komunikace jsou zabezpečeny použitím protokolu TLS.

4.2.2.2 Chat

Chat server musí být nakonfigurován:

- K příjmu XMPP požadavků klient-server Národního Guardu,
- Ke směrování odchozí server-to-server komunikace na Hraniční Guard,
- K příjmu server-to-server požadavků cizích systémů, zaslaných Hraničním Guardem,
- Vyřizování vnitřní komunikace server-to-server za použití Národního Guardu.

Národní Guard musí být nakonfigurován:

- K příjmu XMPP klient-to-server požadavků od připojených uživatelů,
- K příjmu XMPP server-to-server požadavků z chatového serveru,
- Mít schopnost generovat požadavky odchozí komunikace uživatelů na Hraniční Guard,
- K zajištění konektivity k Mechanismu bezpečnostního značkování.

Hraniční Guard musí být nakonfigurován:

- K příjmu XMPP server-to-server požadavků od vlastních i cizích uživatelů,
- Mít schopnost generovat server-to-server směrem k lokálnímu chat serveru i cizím Hraničním Guardům,
- K zajištění konektivity k Mechanismu bezpečnostního značkování.

Veškerá XMPP komunikace je zabezpečeny použitím protokolu TLS.

Mechanismus bezpečnostního značkování dat musí být schopen přijímat XMPP požadavky Národních a Hraničních Guardů a požadavky všech vlastních komponent. Veškerá komunikace prostřednictvím webových služeb je zabezpečena protokolem TLS.

Mechanismus bezpečnostního značkování dat má 4 hlavní části:

- Služby auditu
- Služby ochrany dat
- Správa bezpečnostních značek
- Správa Bezpečnostní Politiky

4.2.2.3 Komunikační infrastruktura

Pro vyšší zabezpečení je vhodné použít segmentovanou síť, tzn. všechny podsítě jsou logicky oddělené (dle schématu). Skutečně fyzicky oddělenými sítěmi je zamezeno nežádoucímu možnému souběhu provozu na lokální síti. Další možností je použití mechanismu směrování síťového provozu MPLS. Nejbezpečnější je však vždy fyzické oddělení sítí.

5 ZÁVĚR

Mechanismus bezpečnostního značkování každé informaci (např. dokumentu) přiřadí tzv. značku. Značka je doprovodný soubor (metasoubor), který obsahuje data a detailně popisuje, jak je povoleno původní informací nakládat. Kdo je adresátem, v jakém stupni utajení může být informace zpracovávána, komu smí být zobrazena a předána.

Řešení využívá tzv. Mechanismus bezpečnostního značkování dat, který je instalován na každé bezpečnostní doméně a obsahuje nastavení bezpečnostních politik jednotlivých domén. Informace jsou v systémech značkovány a je provedeno spojení informace se značkou. Následně je mechanismy zabezpečen bezpečný přenos v rámci systému, nebo do cizího informačního systému. Po přijetí je informace testována (je určena pro národ, je zde odpovídající bezpečnostní politika pro zpracování apod.) a buď vpuštěna do systému, nebo zahozena.

Vzhledem k použitému jazyku pro tvorbu bezpečnostních značek, který umožňuje snadné vytváření konkrétních aplikací pro různé účely a různé typy dat, je jednoduché porovnávat bezpečnostní značky a politiky a tvorba aplikace pro tyto účely není nijak zásadně náročná. Náročná, na implementaci tohoto mechanismu, je filosofie jeho použití a zvláště precizně zpracovaná bezpečnostní analýza organizace. Je nutné do detailu definovat veškeré role, osoby v rolích, jejich funkce a oprávnění a dále probíhající procesy a jejich definice. Pro tyto účely je dobré mít zpracovány jednotlivé architektonické pohledy na informační systém (ať NAF, TOGAF, nebo Zachman) a doplnit je o architekturu bezpečnostní. Je nutné zajistit elektronickou cestou minimalizaci úniku dat při jejich provádění procesů, příp. omezit uživatele natolik, aby nemohl takovou činnost realizovat.

Použití tohoto bezpečnostního řešení je nezbytně nutné pro další rozvoj spolupráce informačních systémů rozdílného stupně utajení. Je-li nutné informace sdílet téměř v reálném čase (chemická situace, polohové zprávy apod.) pak je toto řešení i jediné možné, zvláště z pohledu národních bezpečnostních úřadů jednotlivých národů.

Mechanismus bezpečnostního značkování dat poskytuje vysokou úroveň zabezpečení. Této úrovně je dosaženo převzetím odpovědnosti za tvorbu, ochranu, uložení a distribuce informace. Tato úroveň zabezpečení v kombinaci s dalšími bezpečnostními prvky, jako např. digitální podpis, umožňuje současným vojenským systémům provoz komunikace se systémy civilních organizací (NGO/IZS), za současného dodržení všech bezpečnostních pravidel na ně kladených. Je tím docíleno schopnosti efektivní výměny dat a významného zrychlení elektronické komunikace na místě krize, přírodní katastrofy nebo válečného konfliktu.

6 POUŽITÁ LITERATURA

[1] APIECIONEK, Lukasz, Michal ROMANTOWSKI, Joanna SLIWA, Bartosz JASIUL a Robert GONIACZ. Safe Exchange of Information for Civil-Military Operations. In: *Military Communication Institute* [online]. Warsaw: Military Communication Institute, 2011 [cit. 2016-05-26]. Dostupné z: http://www.wil.waw.pl/art_prac/2011/Safe_Exchange_of_Information.pdf

[2] COOPER, Martin. An introduction to Information Exchange Gateways. In: *Cyber Matters* [online]. Nottingham: Cyber Matters, 2015 [cit. 2016-04-26]. Dostupné z: https://cybermatters.info/2015/01/19/introduction-information-exchange-gateways/

[3] *NATO Information Exchange Gateways: Solution Paper*. Nexor, 2009, 13 s.

[4] *NATO Information Management Policy (ref. a Annex II to PO(99)189)*. b.r..

[5] *Deploying Information Exchange Gateway solutions*. 1. vydání. Nexor, 2015, 2 s. Dostupné také z: https://www.nexor.com/deploying-information-exchan

[6] *Communicating between nations*. 1. vydání. Nexor, 2016. Dostupné také z: https://www.nexor.com/wp-content/uploads/2016/03/Communicating-between-nations.pdf

[7] *Security Label Server*. 1. vydání. ISODE, 2010, 4 s. Dostupné také z: http://www.isode.com/products/security-label-server.html

[8] *Security Policy Infrastructure & Management*. 1. vydání. ISODE, 2012, 5 s. Dostupné také z: http://www.isode.com/products/security-policy-infrastructure.html

[9] HOFFMAN, Peter (ed.). Enhanced Security Services (ESS) for S/MIME. *Internet Engineering Task Force* [online]. 1999 [cit. 2016-05-26]. Dostupné z: http://tools.ietf.org/html/rfc2634

[10] *Xmlspif.org: The home of the Open XML SPIF* [online]. London: xmlspif.org, 2010 [cit. 2016-05-24]. Dostupné z: http://www.xmlspif.org/

[11] DIEPSTRATEN, Martin a Rick PARKER. NATO automated information system co-operative zone technologies. *Journal of Telecommunication anf Information*

Technology [online]. National Institute of Telecommunications, 2004, **2004**(3), 10 [cit. 2016-05-26]. Dostupné z: http://www.nit.eu/publications/journal-jtit

[12] *STANAG 4774: CONFIDENTALITY LABELLING*. 1. vydání. Praha: Úř OSK SOJ, 2014.

[13] JIŘÍ, Kosek. *Inteligentní podpora navigace na WWW s využitím XML*. Praha, 2002. Diplomová práce. Vysoká škole ekonomická. Vedoucí práce Ing. Vojtěch Svátek, Dr.

[14] Simple Mail Transfer Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2016-05-24]. Dostupné z: https://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[15] ZEILENGA, Kurt. XMPP. *XEP-0258: Security Labels in XMPP*. XMPP Standards Foundation, b.r., 51 s. 1.1.

[16] ŠELIGA, Michal, Vladimír MAŘÍK a Pavel JANEČKA. Využití protokolu XMPP pro předávání geografických informací v reálném čase. *Systémová integrace* [online]. Hradec Králové: Česká společnost pro systémovou integraci, 2013, **2013**(2), 11 [cit. 2016-05-25]. ISSN 1804-2716. Dostupné z: http://www.cssi.cz/cssi/vyuziti-protokolu-xmpp-pro-predavani-geografickych-informaci-v-realnem-case

[17] MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. 1. vydání. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 9788074788178.

[18] *STANAG 4778: METADATA BINDING*. 1. vydání. Praha: Úř OSK SOJ, 2015.

[19] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[20] Více úrovňové informační systémy a jejich certifikace podle zákona č.412/2005 Sb., ve znění pozdějších předpisů. *CyberSecurity* [online]. b.r. [cit. 2016-05-26]. Dostupné z: http://www.cybersecurity.cz/data/NBU-MLS

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

7NNN	7 Non NATO Nations
ACL	Access Control List
AČR	Armáda České Republiky
AJP	Allied JOINT Publication
CBRN	Chemical-biological-radiological-nuclear
CIS	Communication Information Systems
CORBA	Common Object Request Broker Architecture
COTS	Commercial-of-the-shelf
CT	Capability Targets
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EU	European Union
FMN	Federated Mission Networking
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection Service
IEG	Information Exchange Gateway
IIOP	Internet InterORB Protocol
IKT	Informační a komunikační technologie
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IS	Informační systém
ISO/OSI	Open Systems Interconnection model
IT	Informační technologie
IZS	Integrovaný záchranný systém
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control Address
MPLS	Multiprotocol Label Switching
MTA	Message Transfer Agent
NAT	Network Address Translation
NATO	North Atlantic Treaty Organisation

NBÚ	Národní bezpečnostní úřad
NC3A	NATO Consultation, Command and Control Agency
NCIA	NATO Communication and Information Agency
NFIP	NATO FMN Implementation Plan
NGO	Non-Govermental Organisation.
NIDS	Network Intrusion Detection Service
NSA	National Security Agency
PfP	Partners for Peace
POP3	Post Office Protocol
RFC	Request for Comments
SDN	Software-defined Networking
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPIF	Security Policy Information File
STANAG	Standardization Agreement
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UDDI	Universal Description Discovery and Integration
URI	Uniform Resource Identifier
VID	VLAN Identifier
WSDL	Web Services Description Language
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

SEZNAM OBRÁZKŮ