Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Umělé imunitní systémy a jejich využití pro filtrování spamu

Bakalářská práce

Autor: Patrik Maisner
Studijní obor: Informační management IM3

Vedoucí práce: Ing. Martina Husáková Ph.D.

Hradec Králové duben 2016

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 27.4.2016

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Martině Husákové Ph.D. za metodické vedení práce.

Anotace

V této práci se autor zabývá problematikou umělých imunitních systémů a jejich aplikací v doméně detekce nevyžádané pošty. Autor zkoumá, jaké jsou v současnosti používané techniky obrany proti spamu a zjišťuje, jakým způsobem lze použít metaforu imunitního systému pro oblast nevyžádané pošty. V této práci je vybrán jeden model reprezentace umělého imunitního systému a podroben analýze. Je zde zkoumána úspěšnost detekce, míra falešných pozitiv i negativ. Z toho jsou vyvozeny patřičné závěry, tedy zda je model schopen úspěšné detekce a pokud ne, co by se mělo na vstupních parametrech či používaných datech změnit. Práce si klade za cíl uvést zájemce do oblasti umělých imunitních systémů, zejména ve spojitosti s detekcí spamu, a prakticky aplikovat vybraný algoritmus umělého imunitního systému pro zjištění nevyžádané pošty.

Annotation

Title: Artificial immune systems and their applications for spam filtering

In this work the author deals with artificial immune systems and their applications on the domain of spam detection. The author examines the currently used techniques of defense against spam and examines how immune system can be used as a metaphor in the field of defense against spam. In this work one method of representation model of artificial immune system is selected and analyzed. Detection rate, rate of false positives and negatives are investigated. From conclusions are deduced information about whether the model can successfully detect spam and, if not, what should be changed on the input parameters and data. Work aims to give basic information to people interested in artificial immune systems and practically apply the selected algorithm artificial immune system to detect spam.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Problematika spamu je v současnosti považovaná za jednu z největších bezpečnostních otázek počítačové bezpečnosti. Neustále se měnící forma i obsah nevyžádané pošty si vyžaduje takové bezpečnostní opatření, které bude schopné přizpůsobovat se neustále se měnícím podmínkám. Umělé imunitní systémy disponují vlastnostmi, které je činí vhodné pro tuto doménu. Z tohoto důvodu bylo toto téma vybráno jako vhodné k hlubšímu prozkoumání a zpracování ve formě bakalářské práce.

V této práci se zabývám problematikou spamu a jeho detekce. Postupně jsou popsány v současnosti používané metody detekce od nejjednodušších až po některé z komplexních metod. S touto oblastí souvisí také oblast umělých imunitních systémů (AIS – ARTIFICIAL IMMUNE SYSTEMS, česky UIS). Aplikace této oblasti na problematiku spamu tvoří těžiště této práce.

V první části práce jsou popsány základy emailové komunikace, resp., kteří aktéři v takové komunikaci vystupují, jaké jsou používané protokoly, a jaký formát samotná zpráva splňuje. Po uvedení základů je popsána problematika spamu. V bakalářské práci je zavedena definice spamu dle zákona a problémy spojené s nevyžádanou poštou. Tyto problémy se týkají jak sociologické tak ekonomické a právní oblasti. Následně jsou zmíněny metody obrany proti nevyžádanému sdělení. Některé z nejvýznamnějších metod jsou v této práci podrobeny analýze. V práci jsou také nastíněny i některé postupy používané útočníky. Umělé imunitní systémy a principy, na kterých tato doména stojí, se popisují v další části. Práce v hrubých rysech zmiňuje vlastnosti a mechanismy fungování imunitního systému člověka, protože jsou inspirací pro různé tzv. imunitní algoritmy, které jsou užívány v mnoha odlišných oblastech. Největší pozornost je věnována algoritmům umělých imunitních systémů, které se týkají oblasti detekce spamu. V další části práce se více rozvíjí myšlenky UIS především v souvislosti s problematikou filtrování spamu. Konkrétní imunitní algoritmus je v práci zanalyzován se zmíněním jeho výhod a nevýhod.

2 Cíl práce

Cílem této práce je aplikovat poznatky z oblasti umělých imunitních systémů na problematiku klasifikace spamu. Výsledkem práce je analýza jedné metody z oblasti UIS používané při detekci nevyžádané pošty. Dalším cílem práce je vytvořit aplikaci, která bude po natrénování schopná určit pravděpodobnost, s jakou lze daný text klasifikovat jako spam. Tato aplikace bude podrobena rozboru efektivity na základě zvolených vstupních parametrů.

Smyslem této práce je aplikovat ne zcela tradiční způsob pro detekci spamu, tj. tzv. algoritmy umělých imunitních systémů, a zároveň vytvořit základ pro zájemce o tuto problematiku.

Otázky položené v této práci jsou následující:

- Jaké jsou základní metody detekce spamu?
- Jakým způsobem lze aplikovat poznatky z oblasti imunitních systémů na problematiku nevyžádané pošty?
- Lze považovat některou z metod z oblasti UIS za použitelnou pro doménu detekce spamu?

3 Základy emailové komunikace

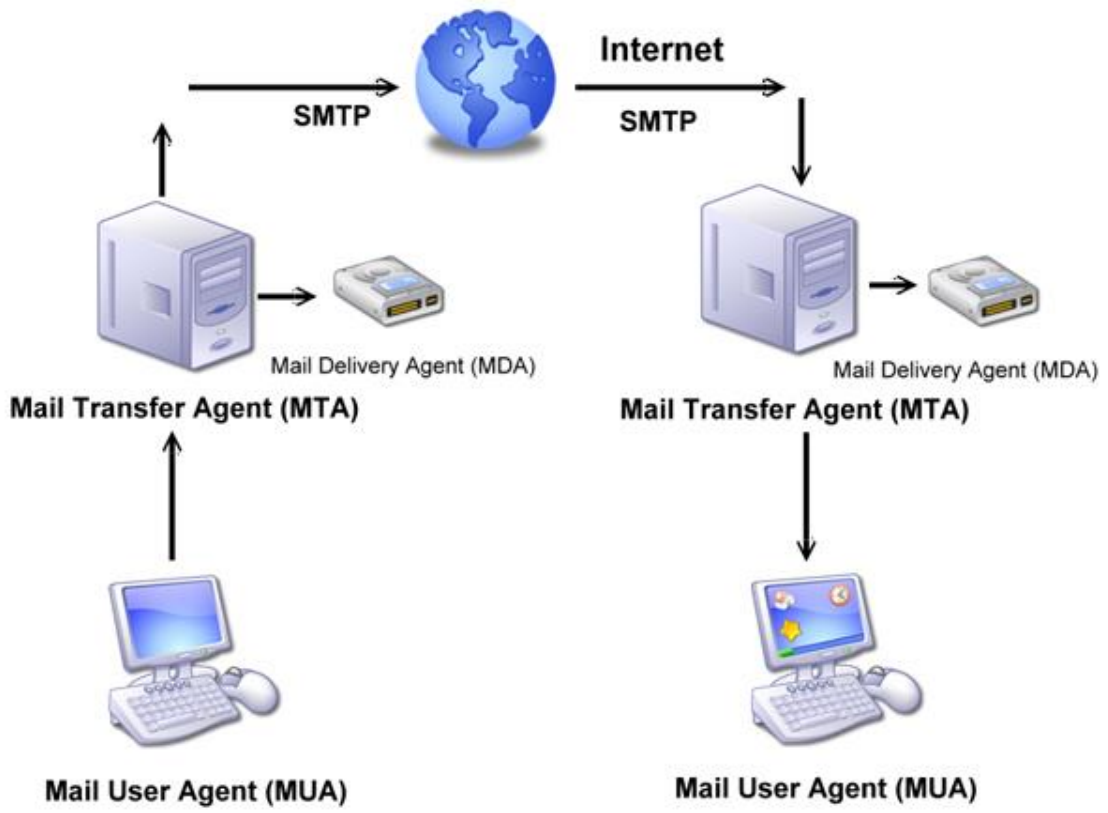
Před rozborem jednotlivých aspektů obrany proti spamu, a některých technik používaných útočníky, je potřeba zavést základní terminologický aparát a vysvětlit způsob, jakým komunikace pomocí elektronické pošty funguje.

Elektronická komunikace, jako způsob výměny informací mezi jednotlivými aktéry, je spojena se samotnými začátky vývoje internetu. Podle dostupných informací se první emailová zpráva přenesla, tehdy ještě v síti ARPANET, v roce 1971. S rozvojem osobních počítačů v 80. letech 20. století nastala revoluce v oblasti komunikace a email se postupně stal základním způsobem komunikace (UMD Department of Computer Science).

Základními stavebními kameny emailové komunikace jsou protokoly SMTP, POP, IMAP a jejich obměny (SMTP protokol existuje dále v rozšířené variantě ESMTP). V této práci budou tyto znaky výměny informací zjednodušeně vysvětleny.

3.1 Architektura

Na následujícím obrázku č. 1 je vyobrazeno schéma popisující cestu emailu internetem. V rámci tohoto náčrtu jsou zřejmí tři aktéři: MAIL USER AGENT, MAIL TRANSFER AGENT a MAIL DELIVERY AGENT.



Obrázek 1 – Zjednodušená architektura zařízení při odeslání emailu (Síťové úložiště (NAS) Synology, 2016)

Každý odeslaný email začíná svoji cestu přes internet na místě tzv. emailového klienta. Na obrázku č. 1 je vyobrazen jako počítač. Anglicky je tento aktér označen jako **MUA** (Mail User Agent). Běžný uživatel emailové komunikace se obvykle dostává do styku pouze s tímto účastníkem provozu. Nejvíce známými zástupci z této kategorie jsou programy Microsoft Outlook, Eudora a jiné. Nevýhodou těchto aplikací je, že po nainstalování se musí nakonfigurovat pro připojení k serveru. Z tohoto důvodu se mnozí poskytovatelé emailových služeb, například Seznam, Google a také Microsoft, rozhodli, že zvýší komfort uživatele pomocí klienta ve webové podobě. K takovému klientovi se stačí připojit pouze

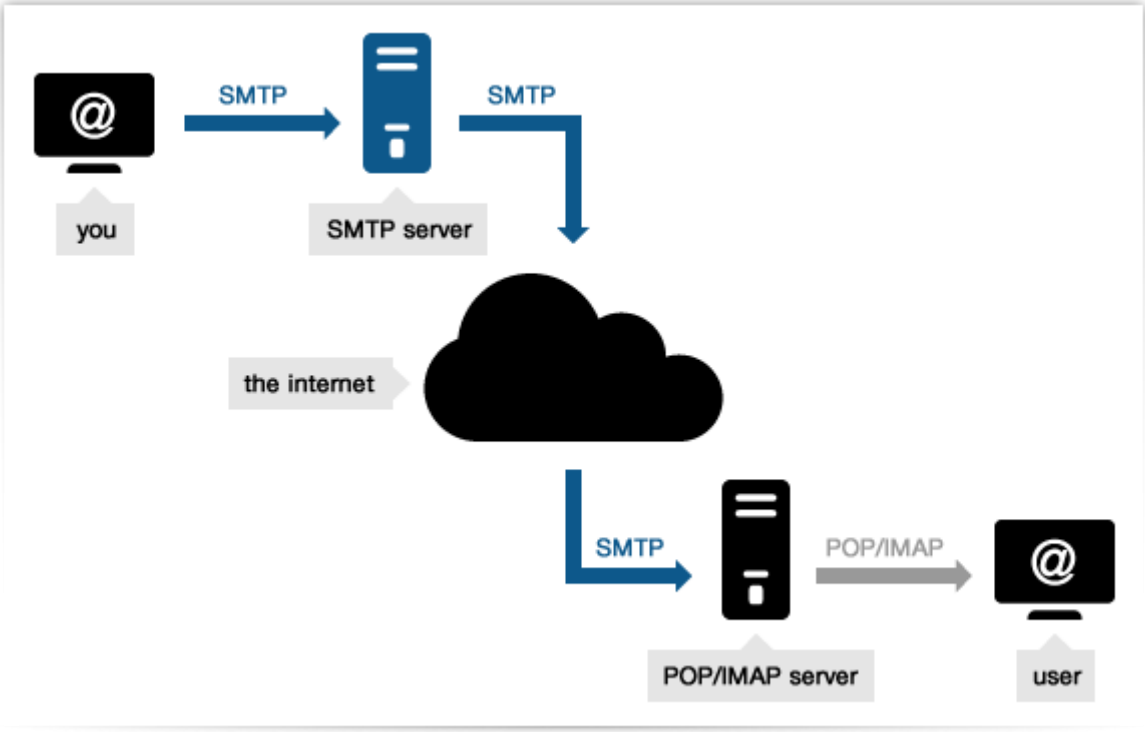
pomocí internetového prohlížeče, zadat přihlašovací údaje, a lze jej užívat bez dalšího nezbytného nastavování (Byers, s. 3).

Po odeslání zprávy z klienta cestuje email k aktérovi, který se anglicky nazývá **MTA**(Mail Transfer Agent). MTA zjednodušeně funguje jako směrovač pro přijaté zprávy. Tento router se při přijetí zprávy podívá na cílovou adresu, konkrétně část obsahující doménu. Pokud se MTA nachází ve stejné doméně, jako je cílová destinace zprávy, pak tuto zprávu pošle datovému úložišti, kde si jen může klient stáhnout. Pokud se ovšem ve stejné doméně nenachází, přichází na řadu proces nazývaný také jako RELAYING. Zjednodušeně se jedná o přeposílání zprávy. Tento proces je probrán v kapitole 3.2.1 o SMTP protokolu. Zástupci aplikací zastávajících úkol směrování jsou například Microsoft Exchange, qmail, Sendmail, Postfix apod,…(Byers, s. 7).

V předchozím odstavci zmíněné datové úložiště se označuje jako **MDA** (Mail Delivery Agent). V této schránce jsou zprávy uloženy pro vyzvednutí emailovým klientem. (Byers, s. 8).

3.2 Protokoly

Na obrázku 2 jsou zobrazeny protokoly použité v každé fázi životního cyklu elektronické pošty. Při posílání emailu přichází na řadu protokol SMTP (nebo jeho obdoba ESMTP). Pro stáhnutí elektronické pošty do emailového klienta se používá protokolů IMAP a POP3. Oba protokoly mají své výhody a nevýhody a svými vlastnostmi se hodí do odlišných situací.



Obrázek 2 – Protokoly při přenosu elektronické pošty (TurboSMTP, 2015)

3.2.1 SMTP - Simple Mail Transfer Protokol

SMTP je základní protokol, pomocí něhož lze odesílat elektronickou poštu v prostředí internetu. V základu se jedná o poměrně jednoduchou soustavu pravidel, kdy jednotlivé příkazy jsou zapsány textově pomocí ASCII kódu, přičemž protokol není citlivý na velikost písmen. To usnadňuje například naprogramování programu Telnet pro automatické odesílání zpráv. Klient navazuje spojení pomocí protokolu TCP na portu 25 a zasílá serveru jednotlivé příkazy, na které server odpovídá pomocí odpovědí obsahující trojciferný stavový kód. Jedním z kódů je například číslo 220, za kterým následuje vlastní adresa serveru. Za použití tohoto trojčíslí se server představuje klientovi (Kabelová et al. 2008, s. 400).

SMTP protokol je definován ve zdrojovém dokumentu RFC-821 (Kabelová et al. 2008, s. 391). Je důležité zde zdůraznit, že tento protokol je spojený výhradně s přeposíláním a zasíláním emailové komunikace v rámci Internetu. Pro získávání zprávy z úložiště na serveru slouží protokoly IMAP a POP3, viz dále kapitoly o IMAP a POP3.

V rámci zasílání pošty funguje proces nazývaný **RELAYING**. Tento děj probíhá v situaci, kdy SMTP server příjme zprávu a zjistí, že adresa příjemce se

nachází na jiné doméně než server samotný. V takovém případě dojde k přeposlání zprávy na adresu, kterou lze dohledat pomocí DNS dotazů na dané doménové jméno.

Dnešní SMTP servery jsou založené na autentizaci, tedy pokud uživatel chce zaslat email, tak musí být přihlášen. Tento proces má za úkol zabránit anonymnímu odesílání údajů od neznámých uživatelů. S přeposíláním pošty pocházející od neověřených serverů je spojen pojem OPEN RELAYING.

Pokud SMTP server přeposílá bez ověření poštu na jiné poštovní servery pak se nazývá **OPEN RELAY**. Jedná se o problém špatné konfigurace, kdy nedochází k ověření odesílatele. Server, který přeposílá zprávy bez ověření se dříve nebo později dostane na černou listinu a jakýkoliv provoz z takového odesílatele bude automaticky zahozen. Proto je velmi důležité SMTP server správně nakonfigurovat (Xeams, 2015).

3.2.2 POP3 – POST OFFICE PROTOCOL

POP3 je jednoduchý protokol, který je specifikován v dokumentu RFC-1939.Pomocí tohoto protokolu si emailový klient může stáhnout přijatou poštu z poštovní schránky na serveru do lokálního úložiště na PC. Stáhnutí do lokálního úložiště umožňuje offline zobrazování a práci s obsahem poštovní schránky. Tento protokol získávání elektronické pošty je užitečný pro jednotlivce, kteří nepotřebují synchronizovat schránku pro více zařízení. Je tomu proto, že tento protokol umožňuje, aby byl uživatel přihlášen ke své poštovní schránce pouze jednou z jednoho zařízení (Kabelová et al. 2008, s. 408-410).

3.2.3 IMAP4 – INTERNET MESSAGE ACCESS PROTOCOL

IMAP4 je protokolem, který je specifikován v dokumentu RFC-3501 a který používá klient pro získání pošty z úložiště na serveru. Oproti POP3 protokolu podporuje možnost synchronizace obsahu emailové schránky mezi více zařízeními. To umožňuje práci s poštovní schránkou z více aplikací najednou (Kabelová et al. 2008, s. 411).

3.2.4 HTTP protokol

HTTP protokol je zde zmíněn okrajově jen pro úplnost. Vystupuje především v komunikaci mezi internetovým prohlížečem a webovým klientem. Problematika HTTP protokolu přesahuje svoji složitostí zadání této práce. Zájemce lze odkázat na (Kabelová et al.2008, s. 361-389).

3.3 Formát emailové zprávy

Struktura poštovní zprávy je jednoznačně specifikována normou RFC-2822. Zpráva obsahuje záhlaví a tělo zprávy, přičemž jsou tyto dvě složky od sebe odděleny prázdným znakem. Obě části jsou tvořeny pouze ASCII znaky. Záhlaví je tvořeno tzv. hlavičkami, které mají jednoznačně daný formát zápisu. Na levé straně figuruje klíčové slovo ukončené dvojtečkou a na pravé straně od dvojtečky figurují parametry. (Kabelová et al. 2008, s. 397-398).

3.3.1 Hlavičky emailu

V rámci dokumentu RFC-822 je specifikován seznam hlaviček a jejich významu. Některé z těchto hlaviček jsou zásadní pro analýzu pošty a rozhodování, zda se jedná o nevyžádanou zprávu. Jiné na druhou stranu figurují pro příjemce jako informace o odesílateli, času odeslání, adrese odpovědi a jiné. Hlavičky jako jsou **To:**, která určuje adresáta a nebo **Date:**, která určuje datum odeslání. Velké části uživatelů bude povědomá hlavička **Subject:**, která popisuje předmět zprávy (Kabelová et al. 2008, s. 398).

Z hlediska zadání práce je zajímavá hlavička **Received:**. Tato hlavička se významnou měrou používá při identifikaci zpětné cesty emailu, což může pomoci určit původce a tedy informaci, zda je zpráva spam či nikoliv. Tato hlavička je přidána na počátek emailu při průchodem každým emailovým serverem. Z toho vyplývá, že tyto hlavičky se čtou odspoda nahoru (pokud chceme zjistit cestu od původce). Některá klíčová slova používaná v této hlavičce jsou následující (Kabelová et al. 2008, s. 398):

- from – počítač, ze kterého byla zpráva přijata (předchozí emailový server)
- by – počítač, kterým byla zpráva přijata (identifikace příjemce)

- via – fyzická cesta
- with – použitý protokol
- id – příjemcova identifikace zprávy
- for – pro koho je zpráva určena

V rámci protokolu jsou definovány i jiné hlavičky, ty ovšem nemají přílišnou důležitost z hlediska tématiky této práce. Pro případné zájemce je seznam některých hlaviček uveden v (Kabelová et al. 2008, s. 398-399).

3.3.2 Tělo emailu

Tělo zprávy obsahuje samotnou zprávu. Nejčastěji se jedná o formát textový nebo HTML. Emailový klient od MS nabízí ještě možnost formátování RTF. Formát HTML v emailu umožňuje přidat do emailu elementy obrázků, odkazů, speciální formátování textu a jiné, které se vyskytují v HTML. S tím je spojeno nebezpečí zneužití. V takovém případě je EMAIL použit jako nosič nebezpečných programů, phishingu atd.

4 Spam

4.1 Definice SPAMU

V době psaní této práce existuje v České republice právní úprava, která řeší spam pouze z obchodního pohledu, jako obchodní sdělení, které není vyžádané. V první části zákon definuje, co je obchodní sdělením. Obchodním sdělením se myslí:

„…všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku osoby, která je podnikatelem nebo vykonává regulovanou činnost.“

Ve stejném zákoně je poté použito této definice pro zavedení pojmu nevyžádaného obchodního sdělení. Zákon říká, že (Zákon o některých službách informační společnosti, § 7 odst. 4 písm. a) až c)):

„Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud:

a) tato není zřetelně a jasně označena jako obchodní sdělení,

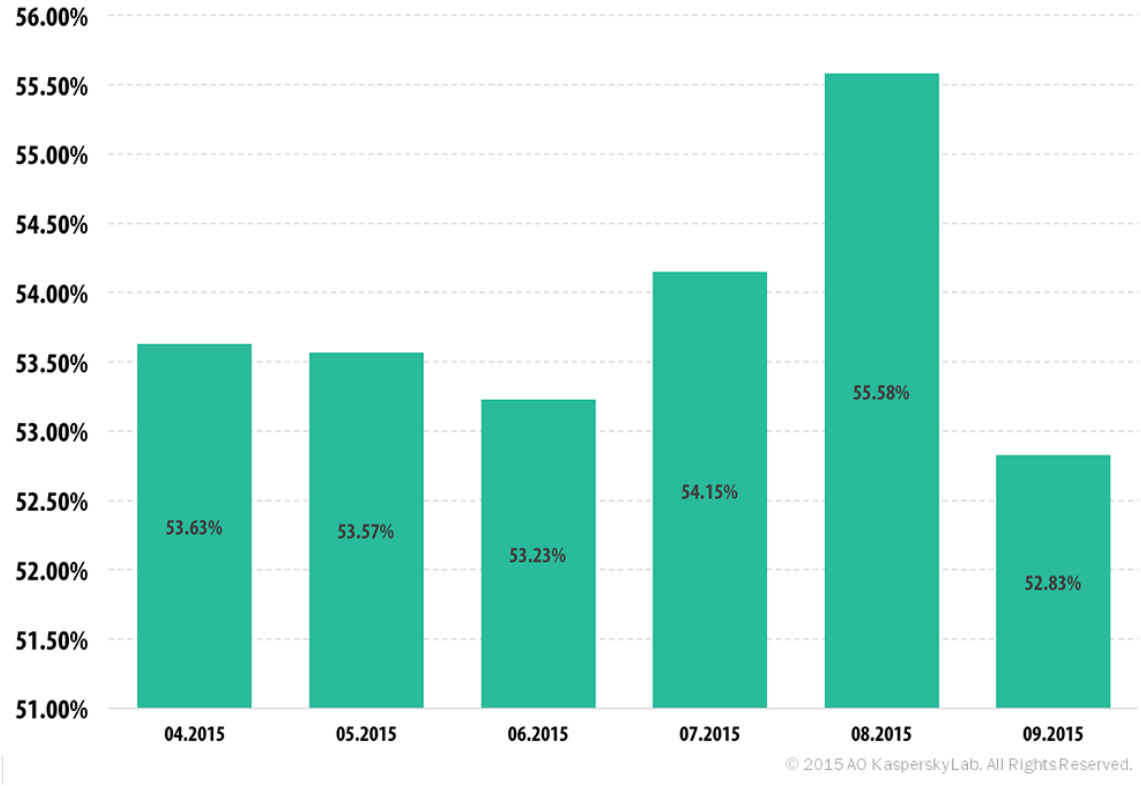
b) skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo

c) je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.“

Podrobnější informace lze získat v (Zákon o některých službách informační společnosti, § 7 odst. 4 písm. a) až c)). Jako dozorčí orgán je určen Úřad pro ochranu osobních údajů. Na stránkách tohoto úřadu lze zaslat pomocí formuláře stížnost, kterou následně tento úřad prošetří (Úřad pro ochranu osobních údajů, 2013).

4.2 Problematika spamu

Spam, neboli nevyžádaná pošta, představuje jeden z nejvýznamnějších problémů spojených s rozšířením vysokorychlostního internetu. Rozesílání emailu je spojeno s nulovými náklady (nepočítaje poplatky účtované od poskytovatele internetového připojení), to činí z tohoto způsobu komunikace ideální prostředek pro zneužití. Dle statistik (Shcherbakova et al. 2015) uveřejněných za třetí kvartál roku 2015 představuje spam okolo 50% z celkového objemu přenesené emailové komunikace, viz obrázek 3.



Obrázek 3 – Objem spamu v odeslané poště (SecureList, 2015)

Problémy spojené ze spamem probíhají v několika úrovních. V prvé řadě masivní rozesílání nevyžádané pošty spotřebovává zdroje, které by mohly být využity jinak. Jedná se o využití sítě, náklady spojené s implementací filtrovacích systémů atd. Kromě samotného problému zneužití zdrojů je velkým problémem bezpečnost. Přes email lze zasílat odkaz na podvodné stránky a také viry. Může docházet i k šíření obchodních nabídek na nelegální produkty.

Velkou část spamu dnes tvoří nabídky na online seznamování, které odkazují na nově vytvořené stránky, viz (Shcherbakova et al. 2015). Propagací se mohou rozesílatelé snažit přesvědčit uživatele k zadání citlivých osobních údajů a platebních informací. Jinou technikou používanou spamery pro obcházení bezpečnostních filtrů jsou PDF přílohy, které v sobě obsahují odkazy pro přesměrování.

Není bez zajímavosti, že podle statistiky na téže stránce je v pořadí první zemí s největším množstvím odesílaného spamu USA. V závěsu jsou země Čína, Vietnam a Rusko.

4.3 Obrana proti spamu

Nyní po definici a uvedení problematiky spojené se spamem se podíváme na metody obrany proti nevyžádané poště. V obecné úrovni se způsoby obrany rozdělují do dvou kategorií. Ty se odlišují na základě fáze přijetí zprávy, ve které operují. Tyto dvě kategorie dělíme na:

- obrana před přijetím zprávy a
- obrana po přijetí zprávy.

Metody před přijetím zprávy analyzují informace o odesílateli a cestě emailu. Na základě toho dojde k rozhodnutí, zda lze považovat zprávu za legitimní či nikoliv. Po přijetí zprávy přichází na řadu metody spojené s klasifikací, pravidly a jiné (Esquivel et al., 2010, s. 40). Oblast klasifikace za pomoci umělých imunitních systémů spadá do této kategorie.

4.4 Obrana před přijetím zprávy

Metody obrany proti spamu z kategorie před přijetím pošty jsou první obranná linie. Nepředstavují stoprocentní obranný mechanismus, pokud jsou ale správně implementovány, mohou značně snížit režii spojenou z analýzou přijatých zpráv na základě jejich obsahu.

4.4.1 Blokování na základě IP adresy

První uvedenou metodou obrany je blokace na základě IP adresy odesílatele, zde SMTP serveru. V nejjednodušší možné podobě se přijímací strana před přijetím emailu podívá do interního či externího seznamu serverů, které byly v minulosti rozpoznány jako rozesílatelé spamu. Pokud se v tomto seznamu nachází i odesílatel, tak je zpráva zahozena. Je zřejmé, že tato metoda není příliš flexibilní, neboť rozesílatelé mnohdy mění servery, které rozesílají. Dalším problémem může být rozesílání pomocí BOTNETU (vytvořená síť počítačů za účelem nelegálních aktivit), kdy může vést blokování na úrovni IP adres až k blokaci celé sítě (Chiou et al. 2013, s. 184-185).

Seznamu serverů, ze kterých se nemá přijímat provoz, se říká tzv. BLACKLIST. Kromě BLACKLIST seznamu existují ještě seznamy WHITELIST a

GREYLIST. WHITELIST seznam eviduje seznam serverů, ze kterých lze přijímat provoz. Pokud není server evidován na WHITELISTU, pak není jeho zpráva přijata. Technika založená na GREYLIST stojí na jednoduchém principu. Každý email, který není uveden v seznamu WHITELIST je odmítnut. Pokud odesílatel svůj pokus bude opakovat za určitý časový interval, potom bude jeho email přijat. Jinak řečeno, SMTP server čeká na druhý pokus (Chiou et al. 2013, s. 184-185).

4.4.2 DNS LOOKUP

DNS LOOKUP nebo také REVERSE DNS LOOKUP je technika pro překlad z IP adresy na doménové jméno. Jedná se o obrácený postup než při běžném překladu doménového názvu na IP adresu při vyhledávání webových stránek prohlížečem. Pro získání doménového jména z IP adresy server zadá požadavek ve speciálním formátu. V tomto formátu je IP adresa zadána v obráceném pořadí a na konec adresy je přidána koncovka in-addr.arpa. Dotaz na IP adresu 77.75.77.53 vypadá 53.77.75.77.in-addr.arpa a odpovědí na tento dotaz je v době psaní práce záznam, ze kterého zjistíme doménový název ***seznam.cz.***

DNS LOOKUP je proces, který tvoří základ silné metody obrany proti rozesílatelům nevyžádané pošty. Jedná se o technikuFCrDNS, viz Kapitola 4.4.3.

4.4.3 Forward Confirmed reverse DNS

FCrDNS je stav sítě, ve kterém jsou si parametry IP adresy a doménového názvu získaného z překladu IP na doménový název a z překladu domény na IP adresu rovny. Pomocí této vlastnosti lze vytvořit slabou formu autentizace, ve které se zjišťuje, zda existuje vztah mezi majitelem doménového názvu a majitelem IP adresy. V rámci obrany proti SPAMU se jedná o silný prostředek validace, viz práce (Chiou et al. 2013, s. 184-185).

4.5 Obrana po přijetí zprávy

Z hlediska zadání této práce je důležitější oblast spojená s klasifikací zprávy na základě jejího obsahu.

4.5.1 Filtrování na základě klíčových slov

Velmi jednoduchá technika detekce nevyžádané pošty. Po přijetí zprávy se vyhledávají klíčová slova, která jsou uvedena v uživateli definovaném seznamu. Každé z těchto slov má přiřazenou určitou hodnou, která definuje, jak často se dané slovo vyskytuje v nevyžádané poště. Při identifikaci slova z databáze ve zprávě se postupně zvyšuje skoré zprávy a pokud překročí určitou hranici, je klasifikována jako nevyžádaná.

Výhoda této techniky je velice snadná implementace takového řešení. Problémem je ovšem flexibilita, kdy každé nové slovo, které rozesílatelé spamu začnou používat, je potřeba do takového seznamu přidat.

4.5.2 Filtrování na základě pravidel

Filtrování na základě pravidel představuje složitější řešení detekce spamu než předchozí příklad stojící na seznamu klíčových slov. Uživatel si ve svém klientovi nastaví pravidla, ať už v podobě klíčových slov či regulárních řetězců, a pokud přijatý email obsahuje dané slovní spojení, pak je zahozen. Může se jednat o pravidla týkající se nejen určitých slov, ale i adresy odesílatele. Jedná se o poměrně efektivní metodu s nižší výpočetní složitosti oproti strojovému učen, která ale ve spojení s dalšími metodami může vydat dobré výsledky. Problém této metody ovšem je, že je potřeba neustále pravidla upravovat a měnit, protože spam se svoji povahou také vyvíjí.

4.5.3 Filtrování na základě kontrolních součtů

Tato obraná technika využívá znalosti, že nevyžádaná pošta je z velké části rozesílaná masově. Email po přijetí na sever je zbaven částí, které se mění (adresa, některé hlavičky a jiné) a zbytek je podroben kontrolnímu součtu (provede se výpočet pomocí HASH funkce. Po výpočtu kontrolního součtu je výsledek porovnán s databází existujících kontrolních součtů pro již identifikovaný spam. Pokud se součet v databázi již nachází, pak je zpráva klasifikována jako nevyžádaná.

Výhodou tohoto způsobu obrany je jednoduchá implementace a v případě masového rozesílání spamu také rychlá reakce (pokud se včas zaeviduje kontrolní

součet do databáze). Nejslabší je z hlediska variability, neboť stačí menší obměna zprávy a kontrolní součet bude kompletně odlišný.

4.5.4 Bayesův naivní klasifikátor

Bayesův naivní klasifikátor představuje jednu z nejvíce efektivních metod detekce spamu na základě obsahu zprávy. Jedná se o klasifikační algoritmus, který lze formálně zapsat takto:

Mějme množinu zpráv $M = \{m_1, m_2, \dots, m_j, \dots, m_{|M|}\}$ a množinu přípustných kategorií $\vartheta = \{spam\,(c_s),\ ham(c_l)\}$. Potom lze zapsat úkol automatizované klasifikace jako pravdivostní funkci$\omega(m_j, c_i) = M \times \vartheta \rightarrow \{pravda, nepravda\}$. Platí, že pokud $\omega(m_j, c_i)$ je pravda, pak m_j patří do kategorie c_i(Almeida et al. 2012, s. 200-201).

Tento klasifikační algoritmus je příkladem strojového učení s učitelem. Probíhá ve dvou fázích více v (Almeida et al. 2012, s. 201):

- Trénování – Algoritmu je poskytnuta množina *M* již klasifikovaných zpráv ve formátu, kterému algoritmus rozumí. Může se jednat o vektor slov, jsou ovšem i jiné reprezentace. Na této množině dat se algoritmus naučí náležitosti spojené se spamem.
- Klasifikace – Po natrénování lze použít klasifikační funkci $\omega(\vec{x}_j)$ pro odhadnutí, zda je daná zpráva spam či nikoliv.

Vektor $\vec{x}_j$ představuje zprávu ve vektorovém zápisu, kde jednotlivé složky představují informaci o výskytu daného slova ve zprávě. Rozklad zprávy na jednotlivé složky se nazývá tokenizace.

Při tokenizaci dochází k rozkladu zpráv na jednotlivé tokeny, obvykle o velikosti jednotlivých slov. Před samotným rozkladem zprávy by ovšem měl být email vystaven korektuře, odebrání stop slov a spojek, které o pravděpodobnosti toho, že je daná zpráva spam, nic nevypoví (Almeida et al. 2012, s. 203).
Výpočet pravděpodobnosti toho, že daná zpráva je spam, proběhne obecně pomocí vzorce:

$$\frac{P(c_s) * P(\vec{x}|c_s)}{P(c_s) * P(\vec{x}|c_s) + P(c_l).P(\vec{x}|c_l)} > T$$

kde T představuje hranici, kterou musí zpráva splňovat, aby byla klasifikována jako spam. Zde je na místě vysvětlit, co znamená slovo naivní v názvu této techniky. Ze vzorce je zřejmý předpoklad, že jednotlivá slova jsou vybírána ze zprávy bez závislosti na jiných, nepředpokládá se tedy žádná vazba ani sémantika, což může vést v některých případech k problémům. Ovšem i přes toto zjednodušení se ukázala tato technika jako efektní.(Almeida et al. 2012, s. 203-204).

V této práci je reprezentována pouze základní forma této techniky. Bayesův klasifikátor existuje v mnoha obměnách, ovšem jejich popis přesahuje zadání této práce. Případné zájemce odkazuji na práci, která se porovnáním jednotlivých obměn tohoto algoritmu zabývá (Almeida et al. 2012).

Výhoda tohoto způsobu detekce je vysoká efektivita a schopnost správně identifikovat příchozí poštu. Problém ovšem vznikne v případě, že data použitá pro trénování nejsou dostatečně spolehlivá. V takovém případě může algoritmus špatně klasifikovat nově příchozí zprávy. Také výpočet pro velké množství zpráv představuje velkou výpočetní zátěž. Tu lze ovšem snížit použitím některé z jednodušších technik, kdy jednoznačný spam je zahozen dříve, než ke klasifikaci nastane.

4.6 Metody útoku

Pro úplnost zde zmíním jen některé metody používané útočníky pro obcházení obrany. Oblast zabývající se metodami útoku na emailové služby je velmi obsáhlá, zasluhující si práci samotnou.

4.6.1 BOTNET

V počítačové bezpečnosti představuje pojem BOTNET stěžejní pojem. Jedná se o síť od desítek až po tisíce počítačů, které jsou ovládány a využívány pro většinou nelegální účely. Nejedná se o jednolitou skupinu, ale jednotlivé druhy se od sebe liší použitým protokolem pro řízení sítě, konkrétně IRC, http, DNS, P2P a jiné (Lashkari 2010, s. 445).

Nyní si uvedeme jednoduchou formální definici. BOTNET představuje skupinu kompromitovaných počítačů. BOTMASTER je zodpovědný za odesílání a přijímání příkazů a kontrolu BOT klientů. BOTY nejsou nic jiného než softwarový program, který činí z počítačů BOTY například stáhnutím softwaru nebo kliknutím na infikovaný email (Lashkari 2010, s. 446).

Problematika BOTNETU je velmi složitá a z hlediska práce nepříliš závazná, proto odkazuji čtenáře na zajímavou přehledovou studii (Lashkari 2010).

4.6.2 Obrázky

S rozšířením používání multimediálního obsahu na internetu se rozšířily možné varianty obcházení detekce spamu. Email se přesunul z čistě textového způsobu komunikace na multimediální, například odesílatelé zprávy mohou do zprávy přidat obrázky. Tato skutečnost umožňuje snáze obcházet již existující textové filtry. Cílem útočníka je vložit do zprávy obrázek či upravit HTML formátování takovým způsobem, aby mohl obejít filtr. Útočník záměrně používá hůře čitelné zprávy v obrázcích, aby znemožnil OCR (OPTICAL CHARACTER RECOGNITION) správně fungovat (Das et al. 2014, s. 129-130).

Pro případné zájemce doporučuji práci (Das et al. 2014), která se touto problematikou zabývá podrobněji.

4.6.3 EMAIL SPOOFING

E-mail SPOOFING je technika popisující aktivitu, při které jsou adresa odesílatele a jiné informace v emailu podvrhnuty tak, aby se zdálo, že přišli z jiného zdroje, než je tomu doopravdy. SPOOFING se používá z mnoha různých důvodů. Může se jednat o vtip mezi jednotlivci, který zpravidla nezpůsobuje žádné hlubší škody. I v takovém případě může jednání v některých zemích nezákonné (Pandove et al. 2010, s. 27).

Hojně se této metody používá při PHISHINGU. Při PHISHINGU se útočník snaží získat informace o daném uživateli (v tomto případě oběti). Některé příklady takové korespondence jsou:

- Email, který tvrdí, že pochází od administrátora a tvrdí, že je potřeba změnit heslo na určitý řetězec
- Email tvrdící, že pochází od autority a požadující heslo.

a mnohé další. Pro další informace odkazuji čtenáře na (Pandove et al. 2010).

5 Umělé imunitní systémy

5.1 Základy imunitního systému člověka

Biologický imunitní systém je robustní, komplexní, adaptivní systém, který chrání tělo před cizími patogeny (organismy, které mohou v těle způsobit nemoc). Je schopen klasifikovat všechny objekty (živé i neživé) v těle jako SELF a NON-SELF (Aickelin et al. 2005, s. 375). Slovem SELF se myslí takové entity, které organismus vnímá jako vlastní. Jsou to některé proteiny a struktury na povrchu buněk, pomocí kterých imunitní systém rozpozná, zda na daný objekt nemá útočit. NON-SELF je na druhou stranu objekt, který lidskému tělu není vlastní. Jsou to cizorodá tělesa, například buňky nebo molekuly.

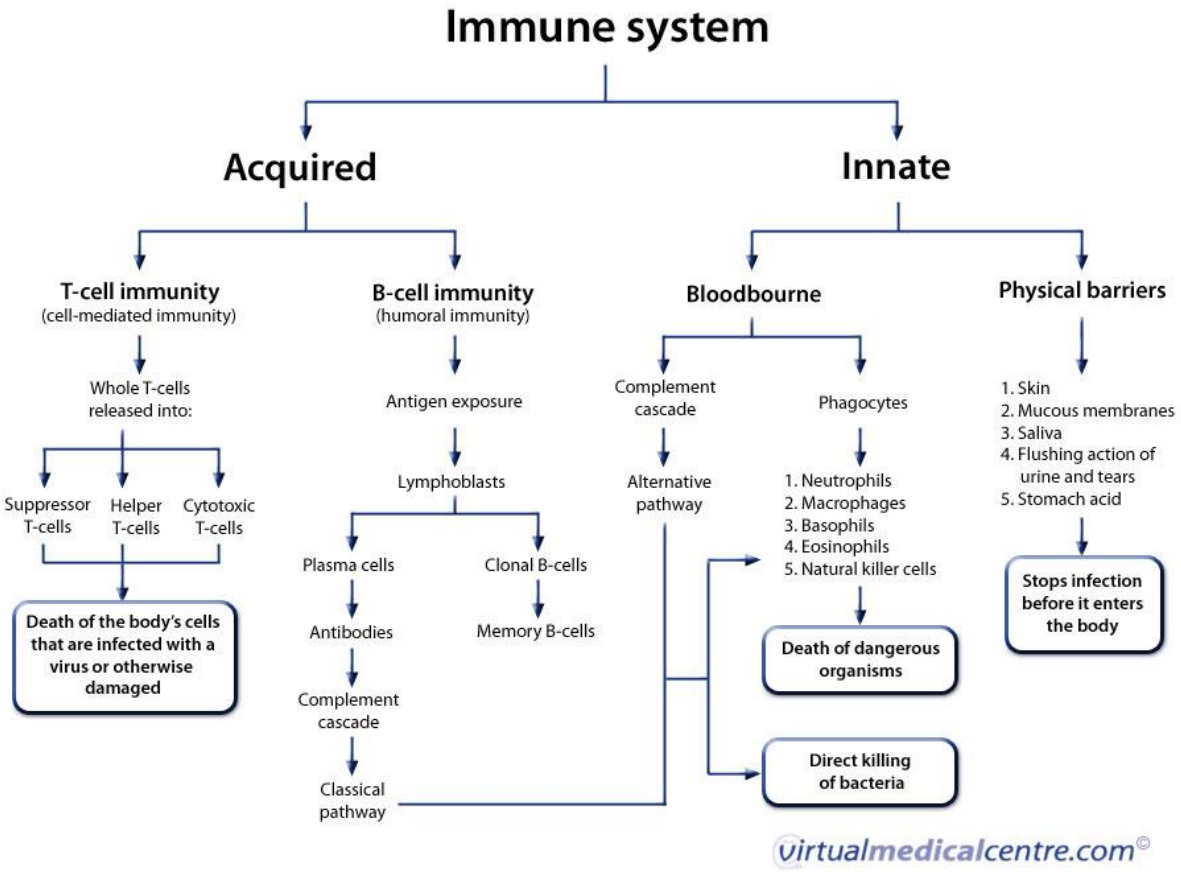
Obrana organismu probíhá v několika úrovních. Jednu úroveň tvoří fyzické bariéry, jako je kůže a respirační systém. Další složku tvoří fyziologické prostředí, konkrétně žaludeční kyselina a destruktivní enzymy. A dále jsou v imunitním systém buňky, které aktivně odstraňují cizorodá tělesa.

Imunitní systém se nejčastěji dělí na specifickou a nespecifickou imunitu. Specifická imunita může být dále rozdělena na buněčnou a humorální. Nespecifickou imunitu má jedinec určenou již od narození. Svou roli v této kategorii obrany hraje fyziologie. Teplota lidského těla, pH a chemické prostředí představují pro některé organismy nevhodné podmínky pro množení. Imunitní systém se dále stará o označení cizích mikroorganismů tím, že je označí protilátkami anebo komplementem (pak se jedná o opsonizaci) a tím usnadní jejich likvidaci makrofágy pomocí fagocytózy, tedy pohlcením (Aickelin et al. 2005 s. 378). Specifická imunita je druhá oblast imunitního systému, která je hlavním zdrojem inspirace pro oblast umělých imunitních systémů. Humorální imunita je tvořena protilátkami v tělesných tekutinách. Funkce tvořit protilátky je spojena s buňkami nazývanými

B-lymfocyty. Ty se, zjednodušeně řečeno, po interakci s antigenem (antigenem je míněno cokoliv, co dokáže způsobit odezvu systému) přemění na plazmatické buňky, které produkují protilátky. Funkce antigenů spočívá ve schopnosti navázat se na receptor buněk a zajistit likvidaci antigenu. Likvidace může být uskutečněna několika způsoby. Protilátka se může navázat na antigen a „zvýraznit“ ho pro fagocytující buňky nebo vytvořit s komplementem komplementový systém, který vede k lýze (rozkladu) organismu (Aickelin et al. 2005, s. 379).

Buněčná imunita je zajišťována T-lymfocyty. Ty můžeme zjednodušeně rozdělit podle funkce na cytotoxické, pomocné a supresorové. Cytotoxické buňky (T_c) si kladou za cíl přímo likvidovat buňky. Pomocné T-lymfocyty (T_h)pomáhají regulovat humorální imunitu. Supresorové T-lymfocyty (T_s)proti alergiím a autoimunitním onemocněním (Aickelin et al. 2005, s. 377). $T_c$likviduje buňky, které jsou antigenem infikovány. $T_h$podporuje imunitu pomocí tvorby cytokinů (molekul, které složí ke komunikaci mezi buňkami), které následně aktivují různé fagocytující buňky, tj. buňky, které mají funkci pohlcovat nebezpečný nebo neužitečný biologický materiál (Aickelin et al. 2005, s. 379).

Na následujícím obrázku je zjednodušené schéma popisující dělení imunitního systému.



Obrázek 4 Dělení imunitního systému (Virtual Medical Centre 2015)

Imunitní systém je komplexním systémem, ve kterém se odehrává celá řada dějů směřovaných k zajištění homeostázy (rovnováhy) organismu. V rámci bakalářské práce jsou zmíněny vybrané procesy, které se staly inspirací pro vývoj algoritmů tzv. umělých imunitních systémů (viz podkapitola 5.4.).

Klonální selekce

Mechanismus klonální selekce je předpokládané chování imunitního systému na antigen. Zjednodušeně říká, že pouze buňky schopné reagovat s antigenem v určité intenzitě se mohou množit (Aickelin et al. 2005, s. 380).

Negativní selekce

Negativní selekce zaručuje, že nově vytvořené buňky imunitního systému budou reagovat jen a pouze na cizorodá tělesa a nebudou napadat buňky vlastního organismu. Při tvorbě T-lymfocytů se receptory tvoří pomocí procesu

pseudonáhodného genetického přeskupování. Po sestavení se v brzlíku vystaví procesu cenzury, který zajišťuje, že buňky organismu vlastní, (SELF), budou zničeny (Aickelin et al. 2005, s. 380). Více v kapitole 5.4.2 o algoritmu negativní selekce.

Teorie imunitních sítí

Teorie imunitních sítí je hypotéza vytvořená v 70. letech pro popis některých vlastností imunitního systému. Tato hypotéza tvrdí, že imunitní systém je tvořen sítí vzájemně propojených B-lymfocytů, které umožňují rozpoznávat antigeny. Tyto lymfocyty se vzájemně mohou stimulovat nebo utlumovat (Aickelin et al. 2005, s. 380). Jinak řečeno, podle této teorie buňky a protilátky imunitního systému nereagují jen na antigen, ale i na sebe navzájem.

5.2 Definice UIS

Imunitní systém člověka disponuje několika vlastnostmi, které jsou velmi výhodné z hlediska informatiky. Proto jej lze využít jako vhodnou a užitečnou metaforu při konstrukci systémů na bázi umělé inteligence. Imunitní systém disponuje některými rysy, které jsou užitečné pro vývoj těchto systémů. Jedná se zejména o rys:

- **samoorganizace** - schopnost systému přizpůsobit svoji vnitřní strukturu vnějšímu prostředí
- **primární a sekundární imunitní odpověď** – Při druhotné odpovědi je systém schopen rychleji reagovat. Disponuje schopností učení a paměti.
- **adaptaci a diverzifikaci** – Schopnost protilátek se vázat nejen na jeden druh antigenu, ale i na antigeny podobné struktury.
- schopnost rozpoznat SELF a NON-SELF

a mnohé jiné, viz blíže např. v (Timmis et al. 2004, s. 62).

Mimo jiné způsoby vymezení se umělé imunitní systémy definují následovně, viz blíže (Timmis et al. 2004, s. 62 - 63):

- *"...an AIS is a computational system based upon metaphors of the natural immune system."*

- *"AIS are intelligent methodologies inspired by the immune system toward real-world problem solving"*
- *"AIS are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving."*

Nyní se podíváme na to, co si představovat pod pojmem FRAMEWORK UIS. Výzkumníci v oblasti UIS si všimli, že jiné větve biologií inspirovaného strojového učení, jako jsou umělé neuronové sítě a genetické algoritmy, disponují v obecné rovině stejnými základními stavebními kameny. Tak jako v umělých neuronových sítích se pracuje s umělými neurony, způsobem jejich propojení a učícím algoritmem, tak v evolučních algoritmech se pracuje s reprezentací jedinců pomocí genů, genetickými variacemi a výběrem. Výzkumníci tedy usoudili, že biologií inspirovaný FRAMEWORK, jakým UIS jednoznačně je, musí obsahovat následující stavební kameny (Timmis et al. 2004, s. 63):

- definici základních stavebních kamenů systému,
- mechanismus pro výpočet interakcí mezi jedinci navzájem a s prostředím,
- proces adaptace, tedy popis toho, jak se systém mění s časem.

Z toho vyplývá, že pokud chceme definovat FRAMEWORK, musíme stanovit tyto základní stavební kameny, ve kterém jsou (Timmis et al. 2004, s. 64):

- stavebními kameny systému jsou jednotlivé buňky imunitního systému a molekuly,
- mechanismus pro hodnocení interakci jsou funkce, které měří afinitu mezi prvky (afinita je intenzita interakcí mezi prvky),
- adaptace a změna prostředí probíhá pomocí obecných algoritmů, jako je např. klonální algoritmus.

Pokud chceme vytvořit systém, musíme definovat aplikační doménu. S tím je spojena reprezentace jedinců v dané problémové doméně. Další na řadě je kvantifikace vztahů, pro kterou se používají jednotlivé míry vzdálenosti, např. Euklidovská a Hammingova vzdálenost. A v poslední řadě se musí sestavit

algoritmus, který bude určovat dynamiku systému. Těmito algoritmy mohou být klonální selekce, negativní selekce, imunitní sítě a jiné (Timmis et al. 2004, s. 64). Jak konkrétně navrhnout UIS se zaměří následující kapitola.

5.3 Návrh UIS

Při implementaci umělého imunitního systému musí být provedeno rozhodnutí o čtyřech aspektech daného návrhu:

- zakódování informace,
- měření afinity,
- výběr entit,
- mutace.

Po rozhodnutí o tom, jakým způsobem se bude kódovat informace, a jakým způsobem se bude měřit afinita mezi prvky, bude daný algoritmus provádět výběr a mutace variant dokud nebude splněno dané kritérium.

5.3.1 Kódování

Protilátka se zapisuje stejným způsobem jako antigen, musí mít stejný formát. Jako první způsob zápisu informace o prvku systému lze uvažovat vektor. Složky tohoto vektoru mohou nabývat hodnot binárních či reálných. Například $\boldsymbol{v} = [1, 0, 0, 0, 1]$ v případě problému o pěti proměnných zapsaných pomocí binárních hodnot (Aickelin et al. 2005, s. 383).

Vektorový zápis informace nelze použít pro každou aplikační doménu. V (Aickelin et al. 2005, s. 383) je uveden příklad domény, ve které informační systém doporučí na základě předchozího hodnocení uživatele nové filmy ke zhlédnutí. V takovém případě je vektorový zápis méně vhodný. Jiným možným zápisem je stanovení škály pro hodnocení filmů od 0 do 5 (0 nejhorší a 5 nejlepší) ve tvaru:

$$Uzivatel = \{\{id_1, score_1\}, \{id_2, score_2\} \dots \{id_n, score_n\}\}$$

kde id_n je identifikátor daného filmu (Aickelin et al. 2005, s. 383-384).
Platí, že zápis informace se velkou měrou odvíjí od povahy aplikační domény.

5.3.2 Měření afinity

Způsob měření afinity závisí na způsobu zapsání informace. Například v případě vektorů $\boldsymbol{v_1} = [0, 0, 0, 0, 0]$ a $\boldsymbol{v_2} = [0, 0, 0, 1, 1]$ budeme měřit tzv. Hammingovu vzdálenost (přesněji opak, měříme afinitu, což je opak vzdálenosti). Ta se spočítá zjištěním, kolik je potřeba změnit znaků v daném řetězci, aby byly řetězce totožné. Zde nám vychází číslo 2 (afinita je 5 – 2 = 3), resp. je potřeba změnit předposlední a poslední prvek. Tento způsob měření afinity může ovšem vést k některým úskalím. Uvažujme dále vektor $\boldsymbol{v_3} = [0,1,0,1,0]$ a spočítejme $D_H(\boldsymbol{v_1}, \boldsymbol{v_3}) = 2$. Ač je vzdálenost totožná jako v prvním případě, vektor $\boldsymbol{v_3}$ má jinou strukturu než vektor $\boldsymbol{v_2}$**.** V některých oblastech použití může být tato skutečnost problematická a je vhodné spočítat afinitu jiným způsobem, třeba pomocí délky nejdelší totožné po sobě jdoucí řady složek mezi dvěma vektory (Aickelin et al. 2005, s. 384). V případě vektoru, který obsahuje složky z oboru reálných čísel, lze spočítat afinitu pomocí geometrické vzdálenosti.

Netradiční aplikační doména, jakou je navrhování filmů z minulé podkapitoly, bude mít speciální způsob výpočtu afinity. V této doméně se snažíme zjistit, který uživatel v databázi má největší podobnost hodnocení filmů. Na základě této informace systém doporučí filmy, které nejsou původním uživatelem hodnoceny, a které druhý uživatel hodnotil kladně (Aickelin et al. 2005, s. 385).

5.3.3 Výběr algoritmu

Výběr algoritmů je podmíněn aplikační doménou. V našem případě je vhodné zjistit, zda budeme používat spíš algoritmus klonální selekce anebo negativní selekce. Například pro oblast výběru doporučeného filmu se spíše hodí klonální selekce, protože se snažíme najít podobného jedince (Aickelin et al. 2005, s. 386).

5.3.4 Mutace

Mutace uvažovaná v umělých imunitních systémech je velmi podobná té z oblasti genetických algoritmů. V případě binárních vektorů se náhodně posouvají a mění bity, v případě reálných hodnot je jedna složka vektoru náhodně změněna. Somatická hypermutace ovšem není vhodná pro všechny oblasti. Například pro oblast doporučení filmů bychom mutováním získali podobné výsledky jako u námi

vybraného uživatele. Problém ovšem je validita takového způsobu zpracování informací a také možnost, že pokud bychom mutování prováděli dostatečně dlouho, získali bychom původního uživatele (Aickelin et al. 2005, s. 388). Nezávisle na několika úskalích je tato vlastnost systému velmi užitečná pro velké množství domén.

5.4 ALGORITMY

Algoritmy z oblasti umělých imunitních systémů a genetických algoritmů jsou druhem evolučních algoritmů s tím rozdílem, že populace se vyvíjí odlišným způsobem. Zatímco v genetických algoritmech je populace tvořena křížením a mutací, v UIS je reprodukce čistě asexuální, každý potomek je přímo klonem svého rodiče. Oba druhy algoritmů ovšem používají mutaci pro udržení diverzity v populaci (Sharma et al. 2011, s. 361).

5.4.1 Algoritmus klonální selekce

Princip klonální selekce říká, že pouze buňky schopné reagovat na daný antigen se mohou množit a tím se vybírají na úkor těch, které na antigen nereagují nebo reagují málo. Tato vlastnost systému je spojena s pojmem imunitní paměť. Organismus si uchovává po prvotní expozici antigenem paměťové buňky a při druhotné expozici je imunitní reakce rychlejší.

Algoritmus klonální selekce, dále už jen CLONALG, je významným zástupcem z rodiny algoritmů inspirovaných imunitním systémem. Princip klonální selekce činní tento algoritmus vhodným pro úkoly spojené s rozpoznáváním vzorů a optimalizaci (Sharma et al. 2011, s. 362).CLONALG disponuje také vlastnostmi, které jej v určité podobě dělají vhodným pro klasifikaci. Pří řešení problému klasifikace vzorku by existovaly obecné paměťové buňky, které by reprezentovaly dané klasifikační třídy. Při kontaktu antigenu s protilátkou je pak klasifikace uskutečněna pomocí výpočtu afinity (Sharma et al. 2011, s. 363).

Algoritmus ve slovní podobě vypadá následovně, viz blíže (Sharma et al. 2011, s. 363 - 364). CLONALG je složen ze dvou množin, množiny protilátek a množiny antigenů. Množina protilátek Ab je dále rozdělena na dvě podmnožiny, Ab_m

jsou buňky paměťové a Ab_r tvoří zbytek buněk (které nejsou považovány za paměťové). Množina paměťových buněk je výstupem toho algoritmu.

Algoritmus:

for Předdefinovaný počet generací

Uvolni antigen: Vyber antigen Ag_i z množiny Ag a vystav ho protilátkám z množiny Ab.

Test afinity: Zjisti afinitu antigenu Ag_i ke každé protilátce z množiny Ab.

Klonuj protilátky: Vyber n protilátek s nejvyšší afinitou a vytvoř množství klonů ke každé této protilátce. Každou protilátku naklonuj v množství proporcionálním k její afinitě. Tím se vytvoří množina klonů C_i.

Maturace afinity: Množina C_i prochází procesem zrání. Každý člen množiny klonů prochází procesem mutace. Daný člen prochází mutací tím více, čím menší afinitu k danému antigenu má (inverzně proporcionálně).

Test afinity: Po procesu zrání vyber z množiny upravených klonů jedince, který má nejvyšší afinitu z množiny C_i. Tento jedinec je kandidát pro vstup do množiny paměťových buněk Ab_m.

Aktualizace paměti: Pokud má kandidát pro vstup do množiny Ab_m větší afinitu než nejlepší jedinec z množiny Ab_m, potom ho nahraď.

Aktualizuj repertoár: Nahraď d nejhorších jedinců v množině protilátek Ab nově náhodně vytvořenými jedinci.

5.4.2 Algoritmus negativní selekce

Negativní selekce představuje další koncept z oblasti imunitních systémů, který zajišťuje, že při generování nových buněk imunitního systému nedojde ke

generování jedinců, kteří by mohli nevhodným způsobem reagovat s organismem. Pro tyto účely je v tomto konceptu definován pojem SELF. SELF je reprezentace objektu, který je systému vlastní, tvoří ho například proteiny vlastního těla. Buňky, které nevhodně reagují na SELF jsou zničeny a do oběhu se dostanou pouze reagující na cizí antigeny (Sahu et al. 2013, s. 771).

Zjednodušeně tento proces probíhá následovně. Při generování T-lymfocytů dochází k pseudonáhodnému genetickému generování receptorů. Po vytvoření tyto receptory projdou cenzurou v brzlíku a ty buňky, které reagují na vlastní proteiny, jsou zničeny (Sahu et al. 2013, s. 772).

Tento mechanismus lze obecně zapsat následovně. V prvním kroku se definuje množina SELF S, která představuje množinu všech normálních stavů daného systému. Množina S je podmnožinou množiny U, která reprezentuje všechny možné stavy daného systému. Ve druhém kroku dojde ke generování množiny detektorů. Pokud libovolný receptor z množiny R detekuje stav z množiny S, pak je zničen. Systém pravidelně monitoruje množinu S pomocí detektorů. Pokud nastane detekce od libovolného detektoru, pak nastala změna v samotném S, neboť detektory jsou naučeny nereagovat pouze na původní SELF (Sahu et al. 2013, s. 772).

Algoritmus negativní selekce je reprezentantem třídy klasifikačních algoritmů. V první fázi dochází k trénování tzv. detektorů a ve druhé dochází ke klasifikaci dat. V této práci je použit zápis přejatý z (Theoretical Biology & Bioinformatics):

Algoritmus

VSTUP:

$S \subset U$ ($množinaSELF$);

$M \subset U$ ($monitorovaná\ množina$)

n ($přirozené$ číslo$značící$ počet$detektorů$)

```
// Trénování
d ← prázdná množina
while |D| < n do
    d ← náhodný detektor
```

```
        if d se neschoduje s žádným elementem z množiny S then
            vlož d do množiny D
        end for
    end while

    // Klasifikace
    for each m ∈ M do
        if m se shoduje s některým detektorem d ∈ D then
            m není SELF (anomálie)
        else
            m je self
        end if
    end for
```

Množina U může pocházet reprezentovat množinu všech UNICODE řetězců, prvky m mohou být emaily a úkolem může být rozpoznání spamu.

Ze zápisu algoritmu lze vyvodit několik negativních vlastností viz (Theoretical Biology & Bioinformatics):

- Pro správnou citlivost může algoritmus požadovat příliš velký počet detektorů n.
- V případě velké množiny S může být výpočetně velmi náročné generovat nové detektory, které se neshodují s žádným elementem z množiny SELF.

6 UIS a Spam

Koncepty z domény imunologie umožňují vytvořit metaforu pro problematiku spamu. Pokud definujeme SELF jako běžný stav, tedy email, který je označený uživatelem jako běžná pošta a NON-SELF jako nesprávný stav, tedy přijetí spamu, pak se nabízí možnost využít algoritmu negativní selekce.

6.1 Implementace programu

Z podkapitoly o návrhu UIS víme, že je potřeba vyřešit čtyři oblasti návrhu. Pro inspiraci byla vybrána práce (Oda et al. 2005).

6.1.1 Kódování

Pro zakódování informace použijeme datovou strukturu lymfocytu, která bude obsahovat dvě proměnné a regulární řetězec. Ten bude porovnáván s danou zprávou a podle shody se budou aktualizovat dvě proměnné. První proměnná bude evidovat počet zpráv, které jsou z části ve shodě s regulárním řetězcem. Druhá proměnná bude evidovat počet zpráv, které byly rozpoznány a které jsou spam. Tyto dvě proměnné poté budou sloužit pro vypočítání pravděpodobnosti, že daná zpráva je spam. Využito k tomu bude váženého součtu podle (Oda et al. 2005, s. 278). Antigen samotný bude reprezentován jako řetězec, tedy celý email se převede do podoby řetězce. Regulární řetězce tvořící molekulární vzorec lymfocytu budou generovány náhodným výběrem z knihovny genetického kódu. Tu bude tvořit seznam jednotlivých regulárních řetězců. Ty se budou náhodně vybírat a spojovat pomocí operátoru (.*), což znamená, že mezi jednotlivými molekulárními vzorci se může vyskytovat žádné až *n* slov. Detekce pomocí regulárních řetězců umožní větší flexibilitu při rozpoznávání klíčových slovních vzorů typických pro spamové zprávy.

6.1.2 Měření afinity

V tomto modelu bude afinita měřená jako schopnost regulárního řetězce se navázat alespoň na jedno místo ve zprávě. Jednotlivé lymfocyty evidují informace o množství zpráv, které jsou schopny rozpoznat a kolik spamu bylo rozpoznáno. Toho je použito dále při měření afinity pomocí váženého průměru. Pokud průměr překročí uživatelem definovaný práh, pak je daná zpráva klasifikovaná jako spam.
Skoré, neboli pravděpodobnost zprávy, že je spam, určíme pomocí následujícího vzorce pro všechny lymfocyty, které jsou schopné se na zprávu navázat.

$$Vážený\ průměr = \frac{\sum_{matchinglymphocytes} spam\_matched}{\sum_{matchinglymphocytes} msg\_matched}$$

Tento způsob výpočtu má své výhody, ale existují i alternativní způsoby výpočtu, viz více v (Oda et al. 2005, s. 280).

6.1.3 Algoritmus

V obecné rovině bude probíhat životní cyklus lymfocytu následovně. Napřed bude vygenerována soustava lymfocytu v počtu definovaném uživatelem. Po generování a inicializaci budou trénovány na množině již klasifikovaných zpráv a poté budou klasifikovat nové zprávy. Nyní budou postupně popsány jednotlivé algoritmy modelu.

Algoritmus 1 – UIS

VSTUP:

```
update_interval ←Délka intervalu, za kterou se bude
populace upravovat (dny, týdny,..)
repertoire ← {Prázdný seznam lymfocytů}
update_time ← current_time + update interval {doba, za
kterou dojde k úpravě populace }

Generuj lymfocyty (algoritmus 2)
Trénuj lymfocyty (algoritmus 3)

whileimunitní systém běží do
     if zpráva je přijata then
          Aplikuj lymfocyty (algoritmus 4)
     end if

     if current time > update_time then
          Odeber lymfocyty (algoritmus 5)
          Generuj nové lymfocyty, aby nahradily původní
     (See Algorithm 2)
          update time ← current_time + update_interval
     end if
end while
```

Tento algoritmus popisuje životní cyklus celého programu. V nejvyšší úrovni dochází napřed ke generování populace lymfocytů s náhodnými antigeny. Ty jsou dále trénovány na data, která již byla předem klasifikována. A poté probíhá samotný režim práce, ve kterém IS čeká na příchozí zprávu. Tu dále klasifikuje. Také průběžně testuje čas, po který běží s tím, že pokud je překročena hranice určená pro obměnu populace, pak budou odebrány ty lymfocyty, které mají nejnižší úspěšnost. A namísto nich je nahradí nově vygenerované.

Algoritmus 2 – Generace lymfocytů

Vstup:

```
library ←knihovna genových fragmentů (nemůže být prázdná)
repertoire ← seznam existujících lymfocytů (může být
prázdný)
p_appending ←pravděpodobnost vazby protilátky (uživatelem
určena)

while repertoire menší než požadovaná velikost populace do
     lymphocyte ← datová struktura s antibody a proměnými.
     antibody ← Náhodně vybraný genový fragment
     lymphocyte.msg_matched ← 0
     lymphocyte.spam_matched ← 0

     repeat
          x ←náhodné číslo od 0 do 1
          whilex < p_appending do
               newgene ←nový náhodně vybraný genový
               segment
               antibody ←Spoj newgene a antobody
               x ← náhodné číslo od 0 do 1
          end while
     until protilátka nemá shodu s žádnou již existující

     lymphocyte.antibody ← antibody
     Přidej  lymphocyte do repertoire
end while
```

Tento algoritmus zajistí vygenerování jedince. V počáteční fázi potřebujeme knihovnu genových fragmentů (v našem případě se bude jednat o seznam regulárních výrazů). Vytvoříme datový objekt lymfocyt, který bude obsahovat informaci o protilátce (jednotlivé regulární výrazy spojené pomocí operátoru (.*), což znamená, že mezi jednotlivými slovy se může vyskytovat 0 až *n* dalších slov. Dále bude tento datový objekt obsahovat informaci o množství rozpoznaných zpráv obecně a antigenů. Poměr

$$\frac{lymphocyte.spam\_matched}{lymphocyte.msg\_matched}$$

bude představovat spolehlivost lymfocytu.

Tvorba samotného řetězce je řízená pravděpodobností. Pro náhodně vybraný gen z genetické knihovny je pravděpodobnost *p_appending,* že bude přidán

na konec. Pokud je pravděpodobnost *x* větší, než tato pravděpodobnost navázání, další gen už není nakonec přidán. V neposlední řadě dojde k testování, zda se nenachází v *repertoire* totožný antigen. Pokud ne, je tvorba lymfocytu završena a populace se rozšíří o nového jedince.

Algoritmus 3 - Trénování lymfocytů

VSTUP:

```
repertoire ← Množina lymfocytů (nemůže být prázdná)
message ← zpráva, která je klasifikovaná jako spam nebo
ham.

if je zpráva klasifikována jako spam then
     spam_increment ← 1
else if je zpráva klasifikována jako ham then
     spam_increment ← 0
else
     spam_increment ← číslo mezi 0 a 1. Pravděpodobnost,
že zpráva je spam.
end if

for eachlymphocytev repertoire
     If lymphocyte.antibodyrozpozná zprávu then
          lymphocyte.msg_matched←lymphocyte.msg_matched +
1
          lymphocyte.spam_matched←lymphocyte.spam_matched
          + spam_increment
     end if
end for
```

Tento algoritmus popisuje samotný proces trénování lymfocytů. Na vstupu tohoto postupu je zpráva, o které je dopředu známo, zda se jedná o spam či nikoliv. Pokud se nejedná o spam, pak je proměnná *spam_increment* nastavena na 0, jinak na jedničku. Toho se později využívá v případě, že spam se naváže na danou zprávu. Pokud se naváže, je počet zpráv, které rozpoznal, zvětšen o jednu. Počet spamových zpráv je zvětšen o inkrement. To znamená, že v případě špatné klasifikace (antigen reaguje na SELF), je počet spamových zpráv stejný. Poměr

$$\frac{lymphocyte.spam\_matched}{lymphocyte.msg\_matched}$$

se tudíž zmenší a s tím se zmenší důvěryhodnost lymfocytu.

Algoritmus 4 – Detekce pomocí protilátek

Vstup:

```
repertoire ←Seznam protilátek
message ←Zpráva na klasifikaci
threshold ←Práh pro určení pravděpodobnosti zprávy, že je
spam.

increment ←Inkrement pro aktualizaci lymfocytů.
Nebo
confidence ←Uživatelem určená hodnota pro důvěru v systém.

Total_spam_matched ← 0 {počet zpráv je inicializován na 0}
total_msg_matched ← 0 { počet zpráv je inicializován na 0}
matching_lymphocytes ← {Inicializuj prázdný seznam
rozpoznávajících lymfocytů}


for each lymphocyte v repertoire do
     if lymphocyte.antibody rozpoznává message then
          total_spam_matched← total_spam_matched +
          lymphocyte.spam matched

          total_msg_matched ←total msg matched +
     lymphocyte.msg matched

          lymphocyte.msg_matched ← lymphocyte.msg matched
     + 1
          Přidej lymfocyt do seznamu rozpoznávajících
     lymfocytů.
     end if
end for


score← lymphocyte.spam_matched / lymphocyte.msg_matched (skoré podle váženého součtu)

if score < threshold then
     Zpráva je spam
     For každýlymfocyte v matching lymphocytes do
          if confidence je určena then
               increment ← confidence * score
          else
               {inkrement byl specifikován uživatelem}
          end if
               lymphocyte.spam_matched ←
               lymphocyte.spam_matched + increment
     end for
```

```
else
     Zpráva není spam.
end if
```

Výše uvedený postup je specifikací samotné klasifikace zprávy. Klasifikace stojí na principu váženého průměru, kdy při klasifikaci zprávy jako spamu je použita hodnota počtu doposud poznaných spamových zpráv daného lymfocytu. Tím dojde k většímu zvětšení pravděpodobnosti, že je daná zpráva spam, v případě, že ji tak identifikují spolehlivé lymfocyty. Dále se spočítá vážený poměr mezi počtem případů, kdy byla zpráva identifikovaná jako spam spolehlivými lymfocyty a kdy byla rozpoznána jako zpráva všemi reagujícími lymfocyty.

Poměr vzniklý z výpočtu je dále porovnán s hodnotou prahu. Pokud tento práh překročí (systém si je jist s větší pravděpodobností, než jaká je vyžadována uživatelem), pak je zpráva klasifikována jako spam a u lymfocytů, které zprávu tak vyhodnotili, se zvětší jejich schopnost určit spam.

Algoritmus 5 – Odebírání protilátek

VSTUP:

```
repertoire← Množina lymfocytů (nemůže být prázdná)
matched_threshold ← Pokud lymfocyt rozpoznal zpráv pod tento
práh, bude smazán
decrement ← míra stárnutí protilátek (zvolená uživatelem)

for each lymphocyte v repertoire  do
     lymphocyte.spam_matched←
```

$$\frac{lymphocyte.spam\_matched}{lymphocyte.msg\_matched} * (lymphocyte.msg\_matched - decrement)$$

```
     {Poměr zůstane stejný i po zmenšení}

     if lymphocyte.msg matched < threshold then
          odeber protilátku ze seznamu
     end if
end for
```

Poslední fází každého průběhu životního cyklu je odebrání těch lymfocytů, které se neukázali jako úspěšné, novými. Toto chování přináší dvě vlastnosti, které jsou z dlouhodobého hlediska přínosné. První vlastností je, že populace nestagnuje, ale přináší se diverzita. Druhou vlastností je, že pokud uživatel změní své preference a některé zprávy, které by nově nebyly uživatelem klasifikované jako spam, bude chtít přijímat, pak je potřeba uskutečnit úpravu populace. Období změny populace může být od hodin až po týdny či měsíce.

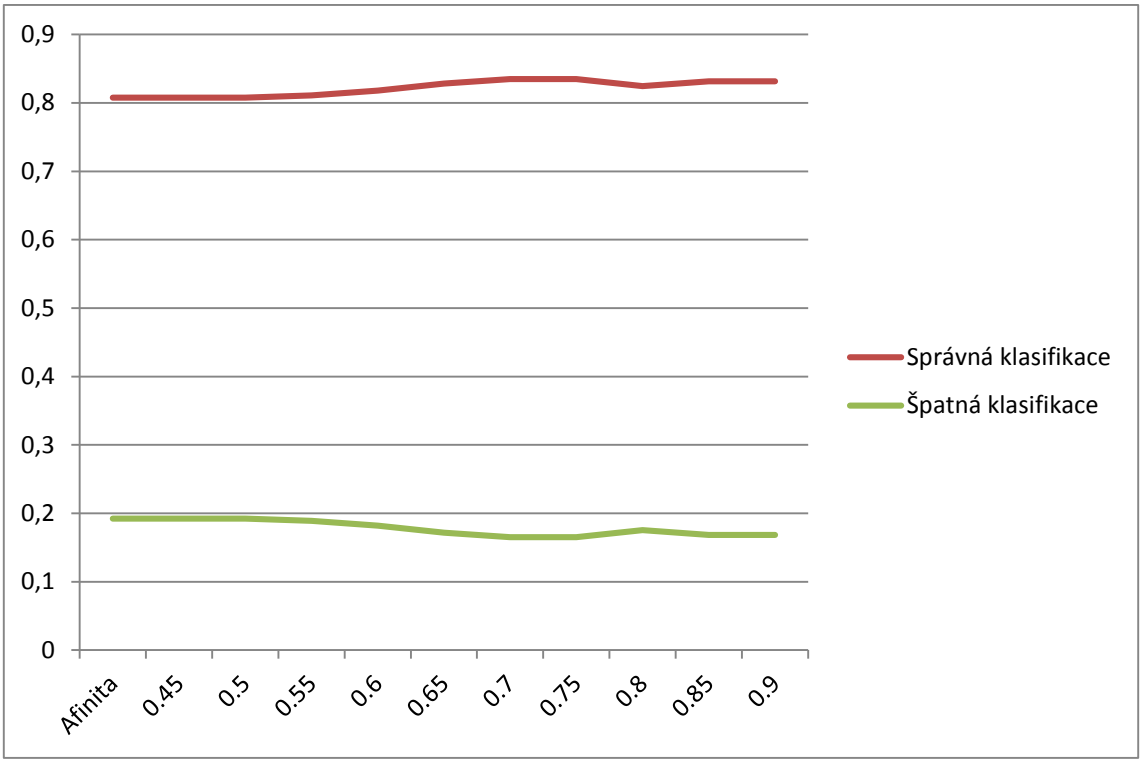
6.1.4 Mutace

Mutace v případě tohoto IS nebude probíhat, neboť implementace mutace regulárních řetězců je značně složitá oblast a přesahuje problematiku této práce.

7 Shrnutí výsledků

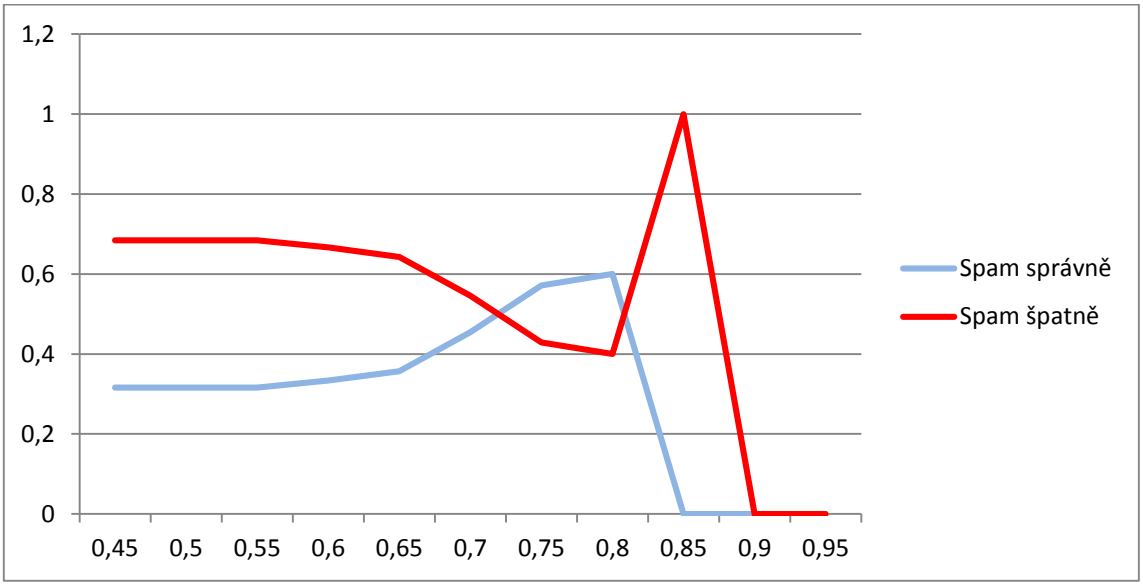
Za použití souboru již klasifikovaných emailů jsme dospěli k rozporuplným závěrům. Implementace programu podle (Oda et al. 2005) obsahuje celkem 201 genových fragmentů, ze kterých generuje protilátky. Knihovnu si vytvořili autoři sami, v této práci byl použit seznam klíčových slov přejatý ze stránky (Chactory 2007), která obsahuje okolo 30 výrazů. Je to zlomek oproti původní práci, což se projevuje i na úspěšnosti detekce. Pro testování jsme použili data volně stažitelná z (Ling-Spam data set). Zprávy z tohoto seznamu emailu obsahují pouze textovou část, hlavičky z nich byly odebrány. V rámci archivu se dále pracuje se složkami, pro tuto práci byla vybrána složka *stop*.

Na následujícím grafu č. 1 si zobrazíme vztah mezi afinitou a podílem správně klasifikovaných zpráv.



Graf 1 - Závislost mezi afinitou a správnou klasifikací

Lze si všimnout, že pravděpodobnost programu správně klasifikovat zprávu se pohybuje okolo 0.8 s maximem při afinitě okolo 0.7. Vzhledem k velikosti knihovny to není špatný výsledek. Zaměřme se nyní na falešně negativní výsledek (správná zpráva je označena nesprávně jako spam).



Graf 2 - Závislost mezi afinitou a falešným pozitivem

Z grafu č. 2 vyplývá, jaká je pravděpodobnost správné klasifikace v případě, že je zpráva označena jako spam. Je zřejmé, že největší pravděpodobnost toho, že zpráva označená jako spam jím opravdu je v případě hodnoty afinity okolo 0.8. V ostatních regionech je pravděpodobnost poměrně nízká a například v případě afinity rovné 0.55 je pravděpodobnost toho, že zpráva označená jako spam jím opravdu, je jedna ku třem. To není příliš pozitivní výsledek. Vyplývá z něho, že program má problém se správným rozeznáním nevyžádaných zpráv. Nyní, když známe relativní hodnoty úspěšnosti, je vhodné podrobit analýze úspěšnost správné identifikace spamu oproti celkovému počtu nevyžádané pošty. Z celkového počtu 49 nevyžádaných zpráv nám v tabulce č. 1 vyšly tyto hodnoty úspěšně označeného spamu.

Afinita	Správně spamu	Celkem spamu	Úspěšnost
0.45	6	49	0.12244898
0.5	6	49	0.12244898
0.55	6	49	0.12244898
0.6	6	49	0.12244898
0.65	5	49	0.102040816
0.7	5	49	0.102040816
0.75	4	49	0.081632653
0.8	3	49	0.06122449
0.85	0	49	0
0.9	0	49	0
0.95	0	49	0

Tabulka 1 - Závislost mezi afinitou a správnou klasifikací spamu

Nyní je zřejmý největší problém aplikace. Je jím velmi nízká úspěšnost identifikace spamu ze seznamu nevyžádané pošty. Spolehlivost okolo 80% v případě úspěšnosti identifikace je dána z velké části tím, že program správně označuje vyžádanou poštu správným způsobem.

Afinita	Správně Ham	Celkem Ham	Úspěšnost
0.45	229	242	0.946281
0.5	229	242	0.946281
0.55	229	242	0.946281
0.6	230	242	0.9504132
0.65	233	242	0.9628099
0.7	236	242	0.9752066
0.75	239	242	0.9876033
0.8	240	242	0.9917355

0.85	240	242	0.9917355
0.9	242	242	1
0.95	242	242	1

Tabulka 2 - Závislost mezi afinitou a správnou klasifikací hamu

Z tabulky č. 2 je zřejmé, že když program identifikuje zprávu jako vyžádanou, tak z velmi velké části se jedná o správné označení. Je vhodné podrobit analýze důvod nízké úspěšnosti identifikace nevyžádané pošty. Hlavní důvod je zřejmý na první pohled. Je jím velikost genetické knihovny. Ve vzorové práci je velikost knihovny 201 genových fragmentů (regulárních výrazů). V práci je použit veřejně dostupný seznam, přičemž počet je blízký 30 fragmentům. To ve velké míře znemožňuje citlivou analýzu, a pokud se některý z výrazu sestavených z genetické knihovny vyskytuje v poště vyžádané i nevyžádané (což v námi vybraném seznamu pošty pro trénování v některých případech je), pak nízká citlivost zkreslí správně výsledek a program může nesprávně identifikovat jako spam i vyžádanou poštu. To se také v tomto případě stalo. Knihovny používané v komerčních programech jsou placeným KNOW-HOW a tudíž není snadné se k nim dostat. Ovšem lze na druhou stranu říci, že i s takto malou knihovou je zřejmá jistá úspěšnost. Lze říci, že za velmi malé knihovny dokáže program identifikovat část nevyžádané pošty a v případě lepší knihovny by se úspěšnost velkou měrou zvýšila. V práci jsme dokázali, že za určitých podmínek může být imunitní systém použit jako funkční metafora pro klasifikaci spamu.

8 Závěry a doporučení

V této práci vytvořený program přinesl jisté výsledky, ovšem oproti původnímu článku nejsou příliš přesvědčivé. Jedním možným řešením by bylo vytvořit si vlastní knihovnu, ze které by se náhodně vybíraly genetické vzory. Rozšířením by pro tuto práci do budoucna mohlo být, že by v ní byl navržen program, který by ze zpráv, označených jako spam, dokázal generovat regulární řetězce pro pozdější potřebu.
Také oblast imunitních systému představuje výpočetně velmi náročnou metodu klasifikace. Ve vlastní práci se autor příliš soustředí na obsahovou složku emailu. Za použití některého přístupu z oblasti obrany proti spamu před přijetím emailu by se mohla snížit režie spojená s klasifikací. Nebo dalším možným rozšířením je vybrat

více než jeden algoritmus a provést porovnání mezi alternativami (ať už z oblasti UIS nebo porovnání s Bayesovým klasifikátorem).

9 Seznam použité literatury

A Brief History of Email. UMD Department of Computer Science [online]. [cit. 2016-04-24]. Dostupné z: https://www.cs.umd.edu/class/spring2002/cmsc434-0101/MUIseum/applications/emailhistory.html

AICKELIN, Uwe a Dipankar DASGUPTA. ArtificialImmune Systems. SearchMethodologies [online]. Boston, MA: Springer US, 2005, s. 375 [cit. 2016-04-09]. DOI: 10.1007/0-387-28356-0_13. ISBN 978-0-387-23460-1. Dostupné z: http://link.springer.com/10.1007/0-387-28356-0_13

ALMEIDA, Tiago A. a Akebo YAMAKAMI. Advances in Spam Filtering Techniques. Computational Intelligence for Privacy and Security [online]. 2012, s. 199 [cit. 2016-04-25]. DOI: 10.1007/978-3-642-25237-2_12. ISBN 978-3-642-25236-5. Dostupné z: http://link.springer.com/10.1007/978-3-642-25237-2_12

BYERS, David. Electronic Mail: PRINCIPLES – DNS – ARCHITECTURES – SPAM. Linköping University. Dostupné také z: https://www.ida.liu.se/~TDDI09/lectures/TDDI09-F4.pdf

DAS, Meghali a Vijay PRASAD. Analysisofan Image Spam in Email Based on ContentAnalysis. International Journal on Natural LanguageComputing [online]. 2014, 3(3), 129-140 [cit. 2016-04-10]. DOI: 10.5121/ijnlc.2014.3313. ISSN 23194111. Dostupné z: http://www.airccse.org/journal/ijnlc/papers/3314ijnlc13.pdf

ESQUIVEL, Holly, Aditya AKELLA a Tatsuya MORI. On the Effectiveness of IP Reputationfor Spam Filtering. In: Communication Systems and Networks (COMSNETS), 2010 Second International Conference on: COMmunicationsystems and NETworks. Piscataway: I E EE, 2010, s. 40-49. ISBN 978-1-4244-5487-7.

Formulář stížnosti - jak podat stížnost na nevyžádaná obchodní sdělení. Úřad pro ochranu osobních údajů [online]. 2013 [cit. 2016-01-31]. Dostupné z: https://www.uoou.cz/formular-stiznosti-jak-podat-stiznost-na-nevyzadana-obchodni-sdeleni/ds-1501/p1=1501

Human Immune System. *Virtual Medical Centre* [online]. 2015 [cit. 2016-04-26]. Dostupné z: http://www.myvmc.com/anatomy/human-immune-system/

CHACTORY. Use the Spam Word Filter to add Regular Expression. *Spamihilator Wiki* [online]. 2008 [cit. 2016-04-26]. Dostupné z: http://wiki.spamihilator.com/doku.php?id=en:tutorials:regex

CHIOU, Pin-Ren, Po-Ching LIN a Chun-Ta LI. Blocking spam sessions with greylisting and block listing based on client behavior. In: . IEEE, 2013, 184 -189. ISBN 978-1-4673-3148-7. ISSN 1738-9445.

KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

LASHKARI, ArashHabibi, SeyedehGhazal GHALEBANDI a Mohammad REZA MORADHASELI. A WideSurvey on Botnet. International JournalofComputerApplications. 2010-8-10, 5(1), 445. DOI: 10.1007/978-3-642-21984-9_38. ISSN 09758887. Dostupné také z: http://link.springer.com/10.1007/978-3-642-21984-9_38

Ling-Spam data set. *Home - CDMC 2016 - Competition* [online]. [cit. 2016-04-26]. Dostupné z: http://csmining.org/index.php/ling-spam-datasets.html

Negative Selection Algorithms. Theoretical Biology & Bioinformatics [online]. [cit. 2016-04-09]. Dostupné z: http://bioinformatics.bio.uu.nl/textor/negativeselection.html

ODA, Terri a Tony WHITE. Immunity from Spam: An Analysis of an Artificial Immune System for Junk Email Detection. Artificial Immune Systems [online]. 2005, s. 276 [cit. 2016-04-24]. DOI: 10.1007/11536444_21. ISBN 978-3-540-31875-0. Dostupné z: http://link.springer.com/10.1007/11536444_21

PANDOVE, Kunal, Amandeep JINDAL a Rajinder KUMAR. Email Spoofing. International Journal of Computer Applications. 2010-8-10, 5(1), 27-30. DOI: 10.5120/881-1252. ISSN 09758887. Dostupné také z: http://www.ijcaonline.org/volume5/number1/pxc3871252.pdf

Reverse IP Lookup - MxToolbox. MX LookupTool - Checkyour DNS MX Records online - MxToolbox [online]. 2016 [cit. 2016-03-02]. Dostupné z: http://mxtoolbox.com/ReverseLookup.aspx

SAHU, Agnika a Prabhat RANJAN MAHARANA. Negative Selection Method for Virus Detection in a Cloud. International Journal of Computer Science and Information Technologies. 2013(4), 771-774. ISSN 0975-9646.

SHARMA, Anurag a Dharmendra SHARMA. Clonal Selection Algorithm for Classification. Artificial Immune Systems [online]. 2011, s. 361 [cit. 2016-04-10]. DOI: 10.1007/978-3-642-22371-6_31. ISBN 978-3-642-22371-6. Dostupné z: http://link.springer.com/10.1007/978-3-642-22371-6_31

SHCHERBAKOVA, Tatyana, Maria VERGELIS a Nadezhda DEMIDOVA. Spam and phishing in Q3 2015.Securelist - Information about Viruses, Hackers and Spam [online]. 2015 [cit. 2016-04-25]. Dostupné z: https://securelist.com/analysis/quarterly-spam-reports/72724/spam-and-phishing-in-q3-2015/

Síťové úložiště (NAS) Synology [online]. 2016 [cit. 2016-01-31]. Dostupné z: https://www.synology.com/cs-

cz/knowledgebase/DSM/tutorial/Application/How_to_make_your_Synology_NAS_a_mail_server

TIMMIS, J., T. KNIGHT, L. N. DE CASTRO a E. HART. An Overview of Artificial Immune Systems. Computation in Cells and Tissues [online]. 2004, s. 51 [cit. 2016-04-10]. DOI: 10.1007/978-3-662-06369-9_4. ISBN 978-3-642-05569-0. Dostupné z: http://link.springer.com/10.1007/978-3-662-06369-9_4

TurboSMTP [online]. 2015 [cit. 2016-01-31]. Dostupné z: http://www.serversmtp.com/en/what-is-smtp

Whatis SMTP relay? Xeams [online]. 2015 [cit. 2016-02-25]. Dostupné z: http://www.xeams.com/smtprelay.htm

Zákon č. 480/2004 Sb., o některých službách informační společnosti. In: Sbírka zákon

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Systémové inženýrství a informatika
Forma: Prezenční
Obor/komb.: Informační management (im3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Maisner Patrik	Zeyerova 715/6, Hradec Králové - Pražské Předměstí	I1300818

TÉMA ČESKY:

Umělé imunitní systémy a jejich využití pro filtrování spamu

TÉMA ANGLICKY:

Artificial immune systems and their applications for spam filtering

VEDOUCÍ PRÁCE:

Ing. Martina Husáková, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

1) Autor se v této práci bude zabývat použitím algoritmů z oblasti umělých imunitních systémů vhodných pro využití v oblasti filtrování nevyžádané pošty, tedy spamu.
2) V první části této práce bude uvedena definice spamu, kategorizace, a také některé v současnosti používané metody pro filtrování nevyžádané pošty.
3) Následně autor uvede teoretické koncepce z oblasti umělých imunitních systémů, základní algoritmy a ukáže, že lze aplikovat koncepce z této oblasti i do oblasti rozpoznávání nevyžádané pošty.
4) Následně budou koncepty, aplikovatelné na tuto doménu rozvinuty a podrobněji popsány, přičemž budou také demonstrovány v praktické ukázce.
5) Výsledkem této práce bude program vytvořený v programovacím jazyce Java, který bude moci umět určit pravděpodobnost, zda daný text je spam.

SEZNAM DOPORUČENÉ LITERATURY:

CASTRO, L. N. and TIMMIS, J., 2002. Artificial Immune Systems: A New Computational Intelligence Approach. London: Springer-Verlag. 357 p. 1st ed. ISBN 1-85233-594-7.

CASTRO, L. N., 2006. Fundamentals of natural computing: basic concepts, algorithms, and applications. Chapman and Hall/CRC, 1st ed., 696 p. ISBN 978-1584886433.

COHEN, I. R., 2007. Real and artificial immune systems: Computing the state of the body. In: Immunology Review, vol. 7, issue 7, pp. 569-574. DOI 10.1038/nri2102.

Podpis studenta: ..... Datum: .....

Podpis vedoucího práce: ..... Datum: .....