



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

VIZUALIZACE SÍŤOVÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

VISUALIZATION OF NETWORK SECURITY EVENTS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR STEHLÍK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PAVEL KROBOT

BRNO 2016

Abstrakt

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v českém jazyce.

Abstract

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v anglickém jazyce.

Klíčová slova

Sem budou zapsána jednotlivá klíčová slova v českém jazyce, oddělená čárkami.

Keywords

Sem budou zapsána jednotlivá klíčová slova v anglickém jazyce, oddělená čárkami.

Citace

Petr Stehlík: Vizualizace síťových bezpečnostních událostí, bakalářská práce, Brno, FIT VUT v Brně, 2016

Vizualizace síťových bezpečnostních událostí

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Pavla Krobota. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....

Petr Stehlík

19. dubna 2016

Poděkování

V této sekci je možno uvést poděkování vedoucímu práce a těm, kteří poskytli odbornou pomoc (externí zadavatel, konzultant, apod.).

© Petr Stehlík, 2016.

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

1	Úvod	3
2	Monitorování sítě	5
2.1	NEMEA	5
2.1.1	Modul	6
2.1.2	Rozhraní	7
2.2	IDEA	7
2.3	Další monitorovací systémy	8
2.4	Shrnutí	9
3	Technologie	10
3.1	Uživatelská část	10
3.1.1	JavaScript MVC frameworky	11
3.1.2	HTML/CSS frameworky	14
3.2	Serverová část	15
3.2.1	REST API	15
3.3	Vybrané technologie	16
3.3.1	Uživatelská část	16
3.3.2	Serverová část	16
4	Architektura aplikace	17
4.1	MVC	17
4.2	Případy užití	17
4.3	REST API	17
4.4	Databáze událostí	17
4.5	GUI	17
5	Implementace	18
5.1	Backend	18
5.2	Frontend	18
5.3	Zabezpečení	18
5.4	Distribuce	18
6	Dosažené výsledky	19
7	Závěr	20
	Literatura	21

Přílohy	23
Seznam příloh	24

Kapitola 1

Úvod

Počítačové sítě, zejména Internet, v dnešním světě zaujímají jednu z nejvýznamnějších rolí. Počínaje výzkumem a vědeckými experimenty, konče běžným životem většiny lidí. Jen za posledních deset let se počet uživatelů Internetu více než ztrojnásobil z přibližně jedné miliardy na tři miliardy uživatelů. Počítačové sítě propoují celý svět a jsou neustále rozšiřovány, vylepšovány a modernizovány. To vede k větším nárokům na použité technologie a zdroje.

Avšak se zvyšujícím počtem uživatelů roste i počet útoků na různé počítačové sítě, kterými se útočníci snaží získat informace či poškodit oběť. Síťový útok je podle [21] definován jako záměrný akt, kde se entita snaží překonat bezpečnostní služby a porušit bezpečnost systému. Současně s tím vznikají systémy na detekci takovýchto útoků, aby správci sítí dokázali včas a efektivně reagovat na vzniklou situaci.

Jeden z těchto systémů vznikl ve sdružení CESNET s názvem NEMEA (Network Measurements Analysis). Tento systém mj. slouží pro analýzu síťového provozu a detekci neobvyklých událostí na síti. Podezřelé toky jako agregované události pak může zaznamenávat do databáze. Na větší síti (stovky až tisíce připojených zařízení) je takovýchto událostí vytvořeno až několik tisíc denně. S tím nastává problém jak dané události jednoduše analyzovat a rozpoznat na jaké události se zaměřit a na které nebrát zřetel.

Pro efektivní analýzu velkého množství dat je vhodná vizualizace dle vhodných metrik, které vyplývají z dostupných dat. Cílem této bakalářské práce je vytvořit aplikaci pro vizuální analýzu bezpečnostních událostí na síti primárně monitorované systémem NEMEA, nicméně díky IDEA formátu dat bude aplikace přenositelná na další systémy.

Důležitým aspektem vytvořené aplikace je důraz na použití moderních knihoven podporující tvorbu dynamických webových aplikací, které jsou dostupné na různých typech zařízeních. Společně s tím je kladen důraz na uživatelskou přívětivost a jednoduchost prostředí, ve kterém bude probíhat vizuální analýza událostí.

Celou aplikaci navíc bude možno libovolně přizpůsobit tak, aby vyhovovala potřebám daného správce sítě. V aplikaci bude zavedena technika *drill-down*, která napomáhá rychlé a přehledné analýze velkého množství dat bez ztráty informací o analyzované události. Drill-down spočívá v postupném zvyšování rozlišení dat, která analyzujeme a postupujeme směrem shora dolů.

Aplikace bude pracovat s konkrétním formátem dat nazvaným IDEA. Tento formát dat je specifikován sdružením CESNET a slouží jako prostředek pro sdílení dat bezpečnostních událostí mezi různými systémy. Díky tomu lze systém kdykoliv přenést na jiný zdroj databáze než je systém NEMEA, např. v rámci sdružení CESNET na systém Warden nebo Mentat.

Aplikace bude integrována do současného NEMEA systému pod názvem NEMEA Dashboard a bude s ním společně distribuována jako front end celého systému.

Kapitola 2

Monitorování sítě

V rozlehlejších sítích jako je např. páteřní či firemní síť je téměř nutností monitorovat a analyzovat provoz na síti, abychom byli informováni o jejím aktuálním stavu, vytížení a zejména negativních vlivech na monitorovanou síť. Samozřejmě i sítě menšího rozsahu by měly být monitorované. Pokud se v malé firmě podaří útočníkovi infiltrovat síť, výsledky útoku mohou být pro firmu likvidační.

Systém pro odhalení průniku (anglicky „Intrusion Detection System“, zkráceně IDS)[18] je takový systém, který analyzuje a identifikuje ze zachyceného provozu podezřelé události. Tyto události může IDS dále klasifikovat. IDS může být dvojího typu.

Prvním typem je detekce anomálií, který má výhodu v možnosti detekce jak známých, tak neznámých útoků. Nevýhodou je, že často může označit normální provoz za útok. Tomu se snaží předejít učením a tvorbou datové sady pro rozpoznání škodlivého provozu.

Druhým typem IDS je detekce založená na pravidlech. Tyto pravidla jsou pevně daná a systém pouze porovnává síťový provoz s danými pravidly. Nevýhodou takového systému je neschopnost detekce neznámých útoků. Některé IDS kombinují oba přístupy a tvoří tak hybridní IDS, který je založen jak na pravidlech, tak na automatické detekci anomálií.

Systém prevence průniku (anglicky „Intrusion Prevention System“, neboli IPS)[18] je narozdíl od IDS aktivním prvkem v počítačové síti. Nejen že detekuje útoky na síť, ale navíc je aktivně blokuje, případně odklání na speciální uzel v síti pro hlubší analýzu útoku.

2.1 NEMEA

Network Measurements Analysis, zkráceně NEMEA, je systém, který umožňuje vytvořit komplexní nástroj pro automatizovanou analýzu toků získaných ze síťového monitoringu v reálném čase. Systém NEMEA je zejména monitorovacím nástrojem, ale slouží také jako IDS.

Systém se skládá z oddělených stavebních bloků nazývané moduly. Tyto jednotlivé moduly jsou následně propojeny pomocí rozhraní TRAP.

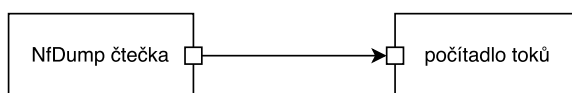
Moduly jsou nezávislé pracovní jednotky, které obecně přijímají proud dat na svých vstupech, zpracují či zanalyzují daná data a následně je odešlou ze svých výstupních rozhraní jako proud dat pro další moduly. Modul může například tvořit statistiky o přijatých datech a na základě těchto statistik detekovat určité typy síťového útoku. Detekovaný útok je popsán datovým záznamem, který je odeslán přes výstupní rozhraní dalším modulům, které s daným záznamem dále pracují, např. jej uloží v IDEA formátu (viz sekce 2.2) do databáze nebo ze získaných statistik dokáží detekovat anomálie v síťovém provozu a dokáží tak

jednotlivé pokusy od jednoho útočníka agregovat a zpracovat jej jako jediný útok skládající se z několika desítek až stovek pokusů o útok v delším časovém intervalu a administrátor sítě by je snadno přehlédl nebo ignoroval, pokud by nebyly agregované.

Jednotlivé moduly se většinou zaměřují na konkrétní typ událostí, případně činnosti. Jejich spojením je možné získat nástroj pro komplexní detekci a analýzu síťových dat schopný detekovat a identifikovat útoky na monitorovanou síť, který následně detekované události uloží do databáze a webová aplikace, kterou v této práci navrhuji, uložené útoky zobrazí.

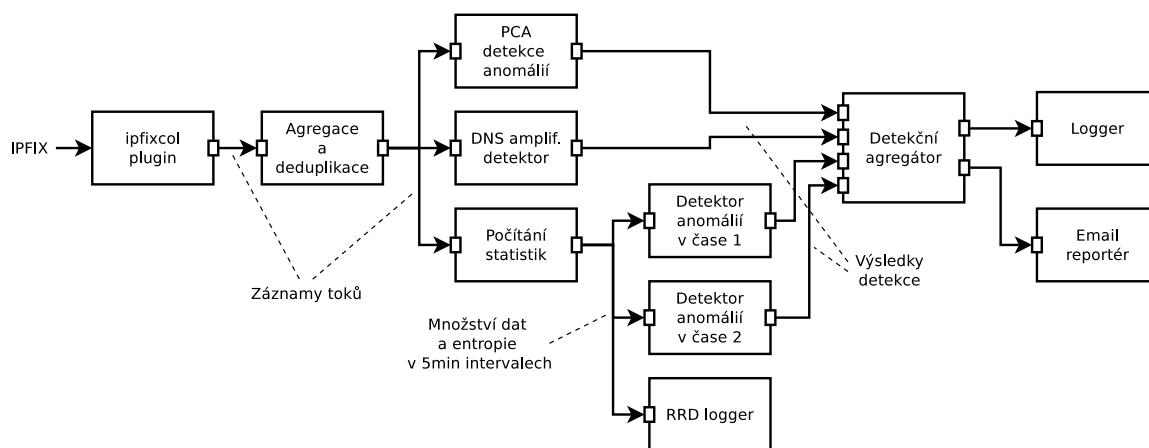
NEMEA je také schopná přístupu „store-and-ex-post“, který lze vidět na obrázku 2.1. Jsou zde dva moduly spojené jedním rozhraním. První modul čte záznamy toků ze souboru a druhý modul počítá statistiky o těchto přečtených tocích. Tento přístup je charakteristický tím jak nakládá se síťovými daty. Ty prvně uloží a až poté začíná systém s analýzou uložených síťových dat.

Oproti proudovému zpracování síťových dat je tento systém náročnější na prostor pro uložení dat, ale analýza je přesnější a méně náročná na výkon stroje, zejména v případě pokročilejší analýzy. Pokud bychom vykonávali proudové zpracování dat, je zde i velká náročnost na operační paměť, pokud chceme analyzovat velké časové rámce.



Obrázek 2.1: Minimální příklad NEMEA systému obsahující pouze dva moduly.

Z takovýchto základních bloků lze postavit i velmi komplexní systém jak je vidět na obrázku 2.2, kde jsou data přijímána v reálném čase z IPFIX[23] kolektoru. Data jsou předzpracována, analyzována několika algoritmy a následně jsou nahlášeny detekované události. Každá z těchto úloh je jeden modul, který může být znovu použitý na několika různých místech.



Obrázek 2.2: Příklad propojení modulů NEMEA systému, který shromažďuje síťová data, detekuje anomálie a útoky a následně události ukládá a reportuje.

2.1.1 Modul

Každý modul je samostatný program nezávislý na ostatních. To sice zvyšuje nároky na systém, ale dovoluje větší variabilitu při návrhu modulu. Ten je, díky tomuto návrhu, možno

naprogramovat v libovolném jazyce, sledovat a řídit spotřebu zdrojů každého modulu zvlášť a zejména v případě nefungujícího modulu se celý systém NEMEA dokáže zotavit z chyby naprosto bez problémů. Modulární systém navíc dovoluje přidávat a odebírat jednotlivé moduly za běhu, což je v produkčním prostředí jedna ze základních vlastností kvalitního monitorovacího systému.

Při zapojení a startu nového modulu se modul periodicky snaží připojit na definované rozhraní. Pokusy o spojení jsou sledovány NEMEA Supervisorem, kterým lze spravovat všechny moduly v systému a pokud se modulu nepodaří po několika pokusech připojit na rozhraní, je modul ukončen.

2.1.2 Rozhraní

Všechny rozhraní jsou výhradně jednocestná a přenos dat je realizován formou jednotlivých záznamů. Všechny záznamy poslané přes jedno konkrétní rozhraní mají vždy stejný formát, nicméně mezi rozhraními se formát může lišit.

Protokol pro dynamickou tvorbu formátu je nazván UniRec. Ten specifikuje nejen formát záznamu, ale také jak záznam vytvořit a jak zpracovat – implementuje formát pro binární reprezentaci síťového záznamu.

Pro tvorbu rozhraní je vytvořena sdílená knihovna libtrap, která využívá Traffic Analysis Platform (zkráceně TRAP) pro komunikaci mezi různými rozhraními a tyto rozhraní využívají protokolu UniRec.

2.2 IDEA

Pro potřebu sdílení informací o síťových událostech mezi různými skupinami a zařízeními (např. honeypoty, analyzéry systémových zpráv, analyzéry provozu na síti, netflow sondy a další) existuje několik formátů záznamu pro takovéto události. Nicméně žádný z nich není natolik univerzální, aby byl vždy a všude použitelný a pokud se k takovému formátu blíží, tak není natolik detailní, aby pokryl všechny důležité informace.

IDEA, neboli Intrusion Detection Extensible Alert, je formát záznamu síťové události specifikovaný sdružením CESNET. IDEA si klade za cíl specifikovat takový formát záznamu, který je univerzální, přenositelný, ale zároveň dost konkrétní a snadno pochopitelný bez potřeby rozsáhlé dokumentace k jednotlivým polím.

Vzorový záznam generovaný systémem NEMEA je vyobrazený ve výpisu 2.1. Jak je vidět, formát je specifikovaný jako JSON dokument, aby byl přehledný, čitelný v běžné podobě (narozdíl od binárních formátů), lehce přenositelný a efektivní (např. oproti XML[17]).

```

{
  "Format" :      "IDEA0",
  "ID" :         "73e0b136-aeb8-4aae-bb80-9bfb4f258847",
  "Category" :   [ "Availability.DDoS" ],
  "Description" : "DNS amplification",
  "EventTime" :  "2016-04-07T22:19:25Z",
  "CreateTime" : "2016-04-07T22:34:52Z",
  "CeaseTime" :  "2016-04-07T22:34:38Z",
  "DetectTime" : "2016-04-07T22:34:38Z",
  "PacketCount" : 393,
  "Source" : [ {
    "IP4" : [ "192.1.0.201" ],
    "Proto" : [ "udp", "dns" ],
    "OutPacketCount" : 393,
    "InPacketCount" : 767
  } ],
  "Target" : [ {
    "Proto" : [ "udp", "dns" ],
    "IP4" : [ "10.0.0.135" ],
    "InPacketCount" : 393
  } ],
  "Node" : [ {
    "SW" : [ "NEMEA", "amplification_detection" ],
    "Name" : "cz.cesnet.nemea.amplification_detection"
  } ],
  "Type" : [ "Flow", "Statistical" ],
}

```

Listing 2.1: Vzorový IDEA záznam ze systému NEMEA. Některé části byly vynechány nebo zkráceny a IP adresy změněny na lokální.

2.3 Další monitorovací systémy

Na trhu jsou v současné době různá dostupná řešení pro detekci a vizualizaci síťových bezpečnostních událostí, nicméně valná hromada z nich je komerční a hlavně vázaná na konkrétní hardware od daného výrobce. Klient tudíž většinou nekupuje software, ale hardware s přiloženým software.

Komerčně dostupný produkt je např. Flowmon[2] ADS[10] od stejnojmenné společnosti. Flowmon je spin-off společností z projektu Liberouter ze sdružení CESNET. Jejich sondy a kolektory využívají technologie vytvořené ve sdružení CESNET jak z hlediska hardware, tak software. Dalším komerčním řešením je Cisco Secure IDS[1], dříve známý jako Cisco NetRanger.

Open source projekty jako NEMEA jsou dostupné mnoho let, ale pouze několik z nich dosáhlo znatelnějšího rozšíření v komunitě síťových správců. Nejvýznamnějšími jsou systémy Snort[20], VERMONT[13] a framework Bro[19].

Snort

Tento open-source projekt, od roku 2013 vlastněn firmou Cisco[3], je možno konfigurovat ve 3 hlavních režimech[4]: „sniffer“, paket logger a jako (N)IDS. V režimu IDS Snort pracuje

principiálně velmi podobně jako systém NEMEA. Zachytává síťový provoz, ukládá si důležité informace o něm a analyzuje jej. Ve výsledku ukládá záznamy o síťových událostech. Nicméně Snort není modulárním systémem a tudíž není tak flexibilní a není stavěný na vysokorychlostní rozsáhlé síti jako systém NEMEA.

VERMONT

VERMONT (Versatile Monitoring Toolkit) je modulární monitorovací systém obsahující IPFIX kolektor, exportér, analyzátor a další moduly a grafické prostředí pro vizuální analýzu dat. VERMONT byl vyvinut v rámci projektu HISTORY[5] a evropským projektem DIADEM firewall[16]. Svou architekturou je nejbližší systému NEMEA, protože je částečně modulární. Systém NEMEA je oproti tomu modulární od samotného jádra systému, což dovoluje vyšší flexibilitu při vývoji a menší závislost na použitých technologiích.

Bro

Dalším v komunitě rozšířeným řešením je framework Bro. Tento framework primárně určený pro síťovou analýzu není podobný systému NEMEA, ani předchozím systémům, protože je to spíše nástroj pro vytváření (N)IDS než-li ucelený systém. Bro se velmi blíží skriptovacímu jazyku (např. Perl) nebo unixovým nástrojům jako tcpdump nebo nfdump. Bro lze rozdělit na dvě vrstvy. První vrstvou je „Bro Event engine“, který analyzuje síťový provoz a generuje neutrální síťové události v podobě „byla vytvořena nějaká událost“.

Tyto neurčité události jsou následně analyzovány druhou vrstvou – „Bro Policy skripty“. V této vrstvě je naimplementovaný zmiňovaný skriptovací jazyk. V současné době existuje mnoho naprogramovaných skriptů, které jsou připraveny k okamžitému použití, včetně pokročilé analýzy síťového provozu.

V ranných fázích vývoje se systém NEMEA velmi blížil frameworku Bro, s vývojem času se ale NEMEA stala uceleným systémem připraveným k okamžitému nasazení na měřicí body.

2.4 Shrnutí

V této kapitole jsme prezentovali systém NEMEA a jeho architekturu. Popsali jsme jeho nejdůležitější části, zejména jak vypadá modul a jeho komunikační protokol. Dále jsme popsali formát záznamu síťové bezpečnostní události IDEA, který je opěrným bodem pro ukládání dat v systému NEMEA v rámci analýzy událostí koncovým uživatelem. V poslední sekci jsme porovnali systém NEMEA s dalšími veřejně dostupnými monitorovacími systémy.

Kapitola 3

Technologie

Vizualizace síťových bezpečnostních událostí může být vytvořena několika postupy. Pokud máme IDS, který je dostupný pouze z jednoho stroje, nejčastěji zvolíme tvorbu desktopové aplikace, protože máme jistotu provozního prostředí jako je např. operační systém, dostupné balíčky a jejich verze, atd. V případě vzdálené správy IDS (častější případ) jsme nejčastěji odkázáni na vzdálený přístup pomocí příkazové řádky. Tento přístup je bohužel velmi limitovaný a nelze jej využít pro vizualizaci. V současné době je pro vzdálenou správu nejvhodnější vytvořit webovou aplikaci, která je dostupná z Internetu a použitelná na většině dnes používaných zařízeních¹

Pro tvorbu moderních webových aplikací je na Internetu dostupná celá řada knihoven, frameworků a systémů. Nicméně první otázkou zůstává co taková moderní webová aplikace je?

Ustáleným pojmem pro moderní webovou aplikaci je z anglického single page application[15] zkratka „SPA“.

Specifikem SPA je její vysoká interaktivita s uživatelem, vysoká dostupnost služby, kterou poskytuje a rozdělení na dva logické celky. Uživatelskou a serverovou část, často chybně nazývané frontend a backend aplikace. Více o architektuře aplikace v kapitole 4.

Většinu z těchto kvalit získává SPA díky způsobu jakým je doručována uživateli. SPA je při prvním načtení stránky v prohlížeči celá uložena v rámci vyrovnávací paměti prohlížeče a během celé doby používání SPA není nutné stránku znova načítat. SPA můžeme chápat jako univerzálního klienta pro obsluhu dané aplikace.

SPA je nejčastěji tvořena pomocí jazyka JavaScript. Ten umožňuje dynamickou změnu stránky bez nutnosti ji znova načítat a tím pádem uživatel nepřichází o dočasná data na stránce. Tento přístup navíc redukuje počet dotazů na server a snižuje tak jeho zátěž.

S přesunem logiky na uživatelskou část SPA jsou ale spojeny nemalé problémy. Zejména pak různorodá interpretace kódu. To se v posledních letech téměř eliminovalo díky moderním prohlížečům a jejich jádrům jako je např. WebKit pro Google Chrome nebo Gecko pro Firefox.

3.1 Uživatelská část

K vytvoření SPA a zejména uživatelské části existuje několik významných systémů. V této části si tyto technologie představíme a porovnáme mezi sebou. Nejdůležitější částí je Ja-

¹Jedná se zejména o stolní počítače, notebooky, tablety a chytré mobilní telefony.

vaScriptová knihovna/framework, který bude nejčastěji interagovat s uživatelem. Další nedílnou součástí je knihovna pro HTML/CSS, která bude definovat vzhled aplikace.

3.1.1 JavaScript MVC frameworky

Bylo vybráno 5 JavaScript frameworků, které napomáhají k tvorbě SPA. Architektura MVC rozděluje aplikaci na tři celky, které mezi sebou navzájem komunikují. Více informací o MVC architektuře v kapitole 4.

Kritéria užšího výběru frameworků byla zejména následující:

- open-source projekt s MIT nebo BSD licencí,
- jednoduché použití,
- relativně nenáročný na výpočetní výkon hostitelského stroje,
- široká podpora mezi prohlížeči,
- projekt má určitou historii a je udržován některou ze známých společností (udržitelnost vývoje).

React[12]

Framework React je vyvíjen pod hlavičkou společnosti Facebook. Původním cílem návrhářů Reactu bylo vyřešit problémy během vývoje komplexních uživatelských rozhraní s rychle měnícími se daty. Dalším cílem bylo vytvořit takový framework, který lze distribuovat v takovém měřítku jako je Facebook.

React je framework pro uživatelskou část SPA používající tradiční MVC architekturu. Taková architektura je nejvíce znatelná v případě použití obousměrného vázání dat (anglicky two-way data binding), více v sekci 4.1.

React se zaměřuje zejména na tvorbu UI, z pohledu architektury pohledová část (view), a kvůli tomu se ostatním částem architektury nevěnuje tak detailně, jak by většinu času vývojář potřeboval. Velmi častým řešením je použít React na pohledovou část a na model a kontrolér použít jiný framework, např. AngularJS.

React pracuje s moderními přístupy k vývoji SPA a boří tak mnoho zažitých technik jak takovou PSA vyvíjet. Místo běžné manipulace s DOM elementy si React, případně vývojář, definuje vlastní DOM elementy, kterým přidává vlastnosti, váže na ně data a manipuluje s nimi bez větších výkonových ztrát. Toho docílil zejména použitím tzv. shadow DOM[24], který je ale novinkou na poli prohlížečů a je podporován pouze jádrem WebKit.

```
var HelloMessage = React.createClass({
  render: function() {
    return <div>Hello {this.props.name}</div>;
  }
});

ReactDOM.render(<HelloMessage name="John" />, mountNode);
```

Listing 3.1: „Hello World“ příklad v jazyku JSX, který do stránky vykreslí text „Hello John“.

Pro názornou ukázkou, jak framework React funguje, je ve výpise 3.1 vytvořen jednoduchý „Hello World“ element v JSX[7] syntaxi. Tento kód demonstruje pouze minimální možnosti frameworku, ale vypovídá o jednoduchosti použití Reactu.

Ember.js

Ember.js je primárně zaměřen na tvorbu SPA. Toho dosahuje zejména používáním zažitých praktik v rámci komunity vývojářů, širokou funkcionalitou bez nutnosti instalace dalších doplňků a osvědčil se i vysokou stabilitou během celé doby vývoje. Ember je také vždy jedním z prvních frameworků, který implementuje novinky obsažené v nových jádrech webových prohlížečů jako jsou např. JavaScript Promises[11], Web Components[26] nebo ES6 syntaxe.

Ember se skládá celkem z pěti klíčových konceptů. Jejich názvy jsou ponechány anglicky pro větší názornost.

- **Routes** – každý stav aplikace je reprezentován unikátní cestou a této cestě náleží i odpovídající objekt, který manipuluje s danou cestou.
- **Models** – každá cesta má svůj korespondující model, který obsahuje data asociována s danou cestou a stavem aplikace. Model slouží zejména k manipulaci s daty.
- **Templates** – šablony jsou tvořeny v HTML s použitím šablonovacího jazyka HTMLBars[6].
- **Components** – komponenta je vlastní HTML značka definovaná programátorem aplikace. Její chování je implementováno pomocí JavaScriptu a její vzhled pomocí HTMLBars šablon. Komponenta se chová jako běžný DOM element.
- **Services** – servis je singleton objekt, který v sobě udržuje dlouhodobá data během používání aplikace klientem.

AngularJS

AngularJS je jedním z nejdéle existujících frameworků pro tvorbu SPA. Je udržován společností Google a poskytuje ucelené prostředí k vývoji komplexních SPA. AngularJS poskytuje dvě metodiky návrhu architektury aplikace. MVC a MVVM (model-view-viewmodel)[22].

MVVM je rozdílný zejména ve způsobu nakládání s daty v aplikaci. Viewmodel pouze reflektuje změny modelu v pohledu a naopak. Viewmodel lze chápat jako interpret dat získaných z modelu, které jsou požadovány v pohledu.

Vzhledem k rozsáhlosti frameworku se nevyhneme tvorbě aplikace, která prolíná oba typy architektury. AngularJS je ale zejména stavěn na základech MVC architektury.

AngularJS staví na několika základních cílech:

- rozdělit manipulaci DOM od aplikační logiky,
- rozdělit klientskou a serverovou stranu aplikace,
- poskytnout strukturu pro vývoj SPA.

Manipulace s DOM je zajišťována v pohledové části architektury. Aplikační logika je v tomto případě oddělena a to dovoluje simultánní tvorbu na obou částech aplikace. To dovoluje strukturovat kód do uzavřených logických celků, které mohou být znovu použity v dalších částech aplikace.

Rozdělením klientské a serverové strany aplikace získává AngularJS celkovou kontrolu nad klientskou stranou a dokáže tak abstrahovat jednotlivé vrstvy aplikace. To dovoluje hlubokou integraci MVC architektury do klientské části.

Toto rozdělení dovoluje frameworku implementovat takové možnosti jako je např. vkládání závislostí nebo pohledově závislé kontroléry.

To vše spěje ke snížení zátěže serveru, na kterém je SPA uložena. Většina, ne-li všechna, aplikační logiky totiž probíhá na klientské straně a server pro svou práci vůbec nepotřebuje. Ten je potřeba až v momentě kdy chceme získat nebo uložit data pro dlouhodobé užití.

Backbone.js

Framework Backbone.js se mírně odlišuje od předešlých a to svou architekturou, která není MVC, ale MVP (model-view-presenter). Presenter je v tomto modelu prostředníkem, který plní logickou funkci a spojuje pohled s modelem. Veškeré akce, které se provedou v pohledu (např. kliknutí na tlačítko) jsou delegovány presenteru. Ten je navíc oddělen od pohledu a komunikuje s ním pouze přes definované rozhraní.

Tento přístup je vhodný zejména pro testování a jasné oddělení jednotlivých částí (zvláště modelu od pohledu). Avšak MVP je náročnější na tvorbu kvůli tomu, že všechny datové vazby musí vytvořit sám programátor.

Výhodou Backbone.js je jeho velikost (celková velikost distribuce je méně než 8 kB) a nezávislost na dalších knihovnách (vyžaduje pouze jednu další knihovnu²).

Z předcházejících faktů lze vyvodit, že Backbone.js je vhodný zejména pro SPA menšího rozsahu, které jsou zaměřeny na velmi konkrétní úkol. To může v pozdějších fázích vývoje SPA znamenat problémy a kompromisy při vývoji další funkcionality aplikace.

Shrnutí

Pro rychlý a stručný přehled byla vypracována tabulka shrnující klíčové vlastnosti každého porovnávaného frameworku.

Tabulka 3.1: Porovnání klíčových vlastností JavaScript frameworků

Název	Verze ³	Aktivní vývoj	Velikost ⁴	Licence
React	15.0.1	3 roky (2013)	142 kB	BSD
Ember.js	2.5.0	4 roky (2011)	450 kB	MIT
Backbone.js	1.3.3	5 let (2010)	7.5 kB	MIT
AngularJS	1.5.3	5 let (2010)	152 kB	MIT

²Underscore.js, pokud chce programátor využít i složité funkce, musí navíc doplnit knihovnu jQuery.

³Aktuální verze v době psaní práce.

⁴Velikost minifikovaného produkčního kódu.

3.1.2 HTML/CSS frameworky

Důležitým aspektem SPA je také její vzhled, nebo spíše UX (user-experience)[8]. UX je zejména vnímání a reakce osoby, které plyne z používání nebo předpokládaného užití/chování výrobku, systému nebo služby. Důraz se musí klást zejména na předpokládané chování systému, tím pádem může uživatel procházet plynule aplikací, aniž by musel odhadovat chování té části aplikace, ve které se právě nachází.

Toho lze dosáhnout zejména uceleností vzhledu a chování jednotlivých komponent SPA. Pro tento účel existují tzv. HTML/CSS knihovny. Na Internetu je jich velké množství a výběr jsem zúžil pouze na 3 knihovny, které jsou známé; mají širokou škálu komponent, které lze v SPA využít a jsou open-source.

Poslední podmínkou jsou zdrojové kódy CSS v jednom z CSS preprocesorů[14] – LESS⁵ nebo SASS⁶, aby v aplikaci byla zaručena konzistence proměnných (např. barvy, velikost, odsazení).

Bootstrap

Bootstrap je nejpopulárnějším frameworkem pro tvorbu vzhledu SPA. Obsahuje HTML a CSS komponenty pro ucelenou typografii, formuláře, tlačítka, navigaci a další. Bootstrap také nabízí komponenty, které jsou částečně nebo zcela napsány v JavaScriptu.

Bootstrap je udržován zejména společností Twitter, kde také vznikl na popud tvorby interních firemních aplikací s uceleným vzhledem a také UX, aby se ušetřily náklady na údržbu takovýchto aplikací.

Díky Bootstrapu se velmi rychle ujal trend responzivního designu a mobile-first přístupu. Navíc disponuje velkou komunitou vývojářů a časté problémy jsou tak mnohokrát vyřešeny.

Foundation

Foundation je velmi podobný framework jako Bootstrap, také nabízí HTML a CSS komponenty pro různé části SPA včetně JavaScript komponent. Nemá sice za sebou takovou společnost jakou je Twitter, ale je neméně kvalitní a udržovaný.

Hlavním rozdílem oproti Bootstrapu je jeho upravitelnost. Foundation dává větší prostor pro úpravu jednotlivých komponent.

Navíc disponuje styly, které jsou automaticky aplikované na dané HTML elementy – vývojář nepotřebuje přidávat množství tříd ke každému elementu. To však nemusí každému vyhovovat a mohou nastat neobvyklé konflikty stylů během vývoje.

Angular Material

Angular Material není běžným CSS frameworkem, nýbrž je velmi úzce spjat s JavaScript frameworkem AngularJS a využívá jeho mnoha možností jako jsou např. vlastní HTML elementy (direktivy).

Framework také obsahuje mnoho HTML a CSS komponent, ale ty jsou vždy velmi úzce spjaty s AngularJS funkcionalitou jako je např. two-way data binding a již zmíněné direktivy.

Společnost Google disponuje vizuálním jazykem pro všechny své produkty nazvaný Material Design⁷. Ten je založený na tzv. „kartičkách“, které lze skládat na sebe, řadit, orga-

⁵<http://lesscss.org>

⁶<http://sass-lang.com>

⁷<https://www.google.com/design/spec/material-design/introduction.html>

nizovat a upravovat.

Jak již název frameworku napovídá je tento vizuální jazyk použit skrz všechny dostupné komponenty.

Z technického hlediska je Angular Material nejpokročilejším frameworkem. Pro mřížkový systém⁸ používá flexbox[25], který je dostupný pouze v nejnovější specifikaci CSS 3 a moderních webových prohlížečích. To může způsobit vážné problémy, pokud je SPA cílena na široké publikum.

3.2 Serverová část

V rámci serverové části je kladen důraz zejména na výkonnost, stabilitu a efektivitu programu. Tyto faktory jsou ovlivněny zejména použitým programovacím jazykem, knihovnami a návrhem architektury programu.

Jediný požadavek na server je, aby byl typu *nix. To nám zaručuje určité faktory a vlastnosti provozního prostředí jako např. dostupné jazyky a jejich knihovny, podpůrné programy a další.

Na serveru poběží z NEMEA Dashboard pouze REST API[9]. Jeho vlastnosti a architektura budou detailně popsány v kapitole 4. API se připojuje na NoSQL databázový systém MongoDB. Ta je využívána systémem NEMEA, který do ní ukládá detekované události. MongoDB bylo zvoleno kvůli rychlosti, jednoduchosti použití a pro záznamy ve formátu IDEA bylo potřeba NoSQL databázový systém, který dokáže pracovat s daty stejně nebo podobně jako se pracuje s JSON.

3.2.1 REST API

REST, neboli Representational State Transfer, je architektura rozhraní pro distribuci dat. Tato architektura nám dovoluje přistupovat ke všem zdrojům uniformním rozhraním, které definuje čtyři základní operace nad každým z nich:

Create – vytvoření a uložení nového datového objektu.

Read – čtení datového objektu.

Update – permanentní aktualizace datového objektu.

Delete – odstranění datového objektu z permanentního datového prostoru.

Toto rozhraní zpřístupňuje databázi událostí vytvořenou NEMEA systémem, která je udržována v MongoDB. Navíc tyto data agreguje, předzpracovává či jinak upravuje (funkcionalita REST API je popsána v sekci 4.3)

Pro vytvoření API s REST architekturou rozhraní existují knihovny, které vývoj ulehčují a zrychlují. Ve většině případů ale platí, že takovéto knihovny jsou náročné na zdroje a jsou tím pádem pomalejší. Pro NEMEA Dashboard je potřeba takový jazyk, který je úzce integrovaný se systémem a dokáže využívat systémové nástroje⁹.

Do výběru jsem zahrnul interpretované i kompilované jazyky, aby byl demonstrován rozdíl ve výkonnosti, jednoduchosti použití, množství potřebných závislostí a dalších. Jmenovitě byly zahrnuty jazyky Python, C++ a JavaScript. Pro každý vybraný jazyk existuje

⁸angl. grid system

⁹Využití systémových nástrojů není součástí této práce, ale byla jednou z podmínek návrhu REST API pro NEMEA Dashboard.

několik knihoven pro podporu tvorby REST API, proto pro zpřehlednění byly vybrány nejvhodnější knihovny.

Jeden z nejpoužívanějších jazyků pro tvorbu webových stránek – PHP nebyl zahrnut z důvodu vysoké režie interpretu při běhu aplikace a mnoha závislostí (zejména Apache webový server), které jsou potřeba pro tvorbu webové stránky v PHP. Navíc jazyk PHP přímo nepodporuje tvorbu REST architektury, vše je řešeno přes Apache server pomocí .htaccess konfigurace.

Flask (Python)

Flask je mikroframework využívající Werkzeug toolkit, který slouží jako základ pro Flask. Je nazývaný mikroframeworkem, protože vývojáře nenutí využívat konkrétní knihovny nebo nástroje, nedisponuje žádnou abstrakční databázovou vrstvou, verifikací vstupů nebo kterékoliv jinou komponentou běžně dostupnou ve frameworku podobného typu.

Nicméně Flask podporuje rozšíření, kterými lze rozšířit funkcionalitu přesně dle potřeb programátora. Tím se stává Flask velmi silným nástrojem při vývoji SPA. Jelikož je navíc napsán v jazyku Python je jeho použití více než intuitivní. Například definice cesty a obslužné rutiny je realizováno pomocí dekorátorů jak je znázorněno v následujícím příkladu [3.2](#).

```
@app.route("/")
def hello():
    return("Hello World!")
```

Listing 3.2: Definování cesty a obslužné rutiny v mikroframeworku Flask.

Veškeré zde zmíněné skutečnosti dělají z mikroframeworku Flask ideální nástroj pro návrh jak rozsáhlého, tak minimálního REST API, které lze libovolně škálovat dle potřeb projektu.

S ohledem na MongoDB existuje oficiální konektor nazvaný PyMongo. Ten se použitím velmi podobá mongo shell nástroji přímo v MongoDB.

NodeJS (JavaScript)

JavaScript je originálně určen do prostředí webových prohlížečů a jejich jader. Google ale vytvořil V8 JavaScriptové jádro primárně určené pro webový prohlížeč, na kterém je ale postaven i framework NodeJS. V8 umožňuje spouštět kód napsaný v JavaScriptu na straně serveru.

Mongoose (C/C++)

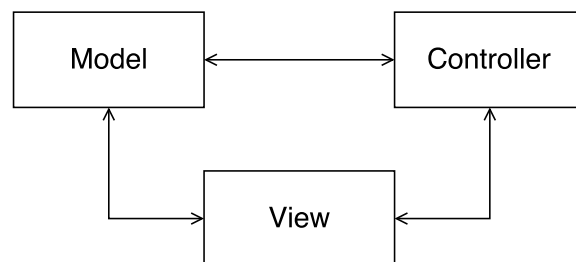
3.3 Vybrané technologie

3.3.1 Uživatelská část

3.3.2 Serverová část

Kapitola 4

Architektura aplikace



Obrázek 4.1: MVC architektura

4.1 MVC

4.2 Případy užití

4.3 REST API

4.4 Databáze událostí

4.5 GUI

Kapitola 5

Implementace

5.1 Backend

5.2 Frontend

5.3 Zabezpečení

5.4 Distribuce

Kapitola 6

Dosažené výsledky

Kapitola 7

Závěr

Závěrečná kapitola obsahuje zhodnocení dosažených výsledků se zvlášť vyznačeným vlastním přínosem studenta. Povinně se zde objeví i zhodnocení z pohledu dalšího vývoje projektu, student uvede náměty vycházející ze zkušeností s řešeným projektem a uvede rovněž návaznosti na právě dokončené projekty.

Literatura

- [1] Carter, E.; Foreword By-Stiffler, R.: *Cisco secure intrusion detection systems*. Cisco Press, 2001.
- [2] Čeleda, P.; Kováčik, M.; Koníř, T.; aj.: FlowMon Probe. *Networking Studies*, 2006: str. 67.
- [3] Cisco Systems, I.: Cisco Announces Agreement to Acquire Sourcefire. 2013.
URL <http://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/sourcefire.html>
- [4] Cisco Systems, I.: Snort Users Manual. 2016.
URL <http://manual.snort.org/node2.html>
- [5] Dressler, F.; Carle, G.: History-high speed network monitoring and analysis. In *Proceedings of 24th IEEE Conference on Computer Communications (IEEE INFOCOM 2005), Miami, FL, USA*, 2005.
- [6] Ember.js: HTMLBars. 2015.
URL <http://emberjs.com/blog/2015/02/07/ember-1-10-0-released.html>
- [7] Facebook: JSX in Depth. 2015.
URL <https://facebook.github.io/react/docs/jsx-in-depth.html>
- [8] FDis, I.: 9241-210 (2009). Ergonomics of human system interaction-Part 210: Human-centered design for interactive systems (formerly known as 13407). *International Organization for Standardization (ISO). Switzerland*, 2009.
- [9] Fielding, R. T.: *Architectural styles and the design of network-based software architectures*. Dizertační práce, University of California, Irvine, 2000.
- [10] Flowmon Networks, a.: Flowmon Anomaly Detection System. 2016.
URL <https://www.flowmon.com/cs/products/flowmon/anomaly-detection-system>
- [11] Foundation, M.: JavaScript Promise. 2016.
URL https://developer.mozilla.org/en/docs/Web/JavaScript/Reference/Global_Objects/Promise
- [12] Gackenheim, C.: What Is React? In *Introduction to React*, Springer, 2015, s. 1–20.
- [13] Lampert, R. T.; Sommer, C.; Münz, G.; aj.: Vermont-a versatile monitoring toolkit for IPFIX and PSAMP. In *Proceedings of the IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation, MonAM*, ročník 6, 2006.

- [14] Mazinianian, D.; Tsantalos, N.: An empirical study on the use of CSS preprocessors.
- [15] Mikowski, M. S.; Powell, J. C.: Single Page Web Applications. *B and W*, 2013.
- [16] Munz, G.; Fessi, A.; Carle, G.; aj.: DIADEM firewall: Web server overload attack detection and response. *Broadband Europe (BBEurope)*, 2005.
- [17] Nurseitov, N.; Paulson, M.; Reynolds, R.; aj.: Comparison of JSON and XML Data Interchange Formats: A Case Study. *Caine*, ročník 2009, 2009: s. 157–162.
- [18] Patil, S.; Rane, P.; Meshram, D. B.: IDS vs IPS. *IRACST–International Journal of Computer Networks and Wireless Communications (IJCNC)*, ISSN, 2012.
- [19] Paxson, V.: Bro: a system for detecting network intruders in real-time. *Computer networks*, ročník 31, č. 23, 1999: s. 2435–2463.
- [20] Roesch, M.; aj.: Snort: Lightweight Intrusion Detection for Networks. In *LISA*, ročník 99, 1999, s. 229–238.
- [21] Shirey, R.: Internet Security Glossary, Version 2. RFC 4949, RFC Editor, Srpen 2007.
URL <https://tools.ietf.org/html/rfc4949>
- [22] Smith, J.: PATTERNS-WPF Apps With The Model-View-ViewModel Design Pattern. *MSDN magazine*, 2009: str. 72.
- [23] Velan Petr, K. R.: Flow Information Storage Assessment Using IPFIXcol. In *Lecture Notes in Computer Science 7279*, Springer, 2012, ISBN 978-3-642-30632-7.
- [24] W3C: Shadow DOM. Working Draft. 2015.
URL <http://www.w3.org/TR/shadow-dom/>
- [25] W3C: Flexible Box Layout Module Level 1. Candidate Recommendation. 2016.
URL <http://www.w3.org/TR/css-flexbox-1/>
- [26] WebComponents: Web Components. 2016.
URL <http://webcomponents.org/>

Přílohy

Seznam příloh