Univerzita Pavla Jozefa Šafárika v Košiciach

Prírodovedecká fakulta

ČASOVÉ HĽADISKO V KYBERNETICKEJ BEZPEČNOSTI

BAKALÁRSKA PRÁCA

Študijný odbor: **Informatika**
Školiace pracovisko: **Ústav informatiky**
Vedúci záverečnej práce: **RNDr. JUDr. Pavol Sokol, PhD.**
Konzultant: **RNDr. Andrej Gajdoš**

Košice 2019

Radovan Fuska

Poďakovanie

Rád by som poďakoval môjmu vedúcemu RNDr. JUDr. Pavlovi Sokolovi, PhD. za ochotu, pomoc a trpezlivoať a konzultantovi RNDr. Andrejovi Gajdošovi za cenné pripomienky pri vypracovávaní tejto bakalárskej práce.

Univerzita P. J. Šafárika v Košiciach
Prírodovedecká fakulta

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Radovan Fuska
Študijný program: Informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: 9.2.1. informatika
Typ záverečnej práce: Bakalárska práca
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Časové hľadisko v kybernetickej bezpečnosti

Názov EN: Temporal view in the cyber security

Cieľ:
1. Analýza štatistickým metód využívajúcich časové hľadisko v kybernetickej bezpečnosti.
2. Porovnanie aktuálnych prístupov k predikcii kybernetických bezpečnostných incidentov.
3. Návrh, implementácia a vyhodnotenie systému na predikciu kybernetických bezpečnostných incidentov.

Literatúra:
1. WERNER, Gordon; YANG, Shanchieh; MCCONKY, Katie. Time series forecasting of cyber attack intensity. In: Proceedings of the 12th Annual Conference on Cyber and Information Security Research. ACM, 2017. p. 18.
2. BOX, George EP, et al. Time series analysis: forecasting and control. John Wiley & Sons, 2015.
3. LIU, Yang, et al. Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In: USENIX Security Symposium. 2015. p. 1009-1024.
4. ESLING, Philippe; AGON, Carlos. Time-series data mining. ACM Computing Surveys (CSUR), 2012, 45.1: 12.

Vedúci: RNDr. JUDr. Pavol Sokol, PhD.
Konzultant: RNDr. Andrej Gajdoš
Ústav : ÚINF - Ústav informatiky
Riaditeľ ústavu: prof. RNDr. Viliam Geffert, DrSc.

Dátum schválenia: 03.05.2019

Univerzita Pavla Jozefa Šafárika v Košiciach
Prírodovedecká fakulta
Ústav informatiky

Abstrakt

Kybernetická bezpečnosť, resp. informačná bezpečnosť je v súčasnosti veľmi aktuálnou témou. Problematika bezpečnosti je veľmi rozsiahla a obsahuje niekoľko uhlov pohľadov - spôsobov na riešenie bezpečnostných problémov. V tejto práci sme sa zamerali na tie spôsoby riešenia problémov, ktoré využívajú pri riešení časový aspekt. K tomuto účelu sme súčasne porovnali a analyzovali aktuálne spôsoby predikcie kybernetických útokov. Použili sme ako dataset záznamy zo systému WARDEN od skupiny CESNET. Z nich sme vytvorili časové rady kvantity záznamov agregovaných podľa kategórií, portov a protokolov jednotlivých zázanmov v pravidelných intervaloch. Na týchto radoch sme otestovali štyri metódy na predikciu. Na záver sme vyhodnotili najlepšie metódy podľa presnosti ich predikcií.

Kľúčové slová: *kybernetická bezpečnosť, kybernetické útoky, informačná bezpečnosť, počítačová bezpečnosť, bezpečnosť, časové rady, predikcia*

Abstract

Cyber security, or information security, is nowadays a very topical subject. The issue of security is very broad and encompasses multiple view points - methods for solving security problems. In this work we focused on methods which utilise time aspect. For this purpose we simultaneously compared and analysed current methods of predicting cyberattacks. We used as a dataset records from system WARDEN by CESNET group. From it we created time series of quantity of records aggregated by category, port and protocol of each record in regular intervals. We tested four prediction methods on these series. In conclusion we evaluated the best methods based on the accuracy of their predictions.

Keywords: *cyber security, cyber attack, information security, computer security, security, time series, forecasting*

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

V súčasnej dobe predstavuje kybernetická bezpečnosť prirodzenú súčasť každodenného života menších aj väčších organizácií. V rámci realizácie bezpečnosti organizácie, organizácie vykonávajú proaktívne a reaktívne činnosti. Účelom proaktívnych činností je predchádzať bezpečnostným incidentom, teda znižovať pravdepodobnosť ich výskytu. Naproti tomu, reaktívne činnosti sú zamerané na riešenie už vzniknutých bezpečnostných incidentov. Ich účelom je minimalizovať čas na riešenie bezpečnostného incidentu a dopad týchto incidentov na samotnú organizáciu.

Medzi proaktívne činnosti organizácie môžeme zaradiť aj monitorovanie vlastnej sieťovej infraštruktúry vrátane sieťových služieb a informačných systémov v nej obsiahnutých. Takéto monitorovanie nám poskytuje veľké množstvo cenných údajov, ktoré je možné využiť v rámci analýzy správania sa konkrétnych útokov, resp. útočníkov.

V rámci tejto záverečnej práce sa venujeme možnosti využitia zozbieraných údajov z dohľadových a bezpečnostných systémov. Každý takýto bezpečnostný údaj obsahuje časový údaj. Z tohto dôvodu, časové hľadisko v tomto smere hrá významnú rolu. V rámci práce sme si stanovili tri výskumné ciele. Prvým cieľom je analýza štatistických metód použitých na predikciu bezpečnostných udalostí použitím časových údajov obsiahnutých v bezpečnostných údajoch. Druhým cieľom je analýza a porovnanie aktuálnych prístupov k predikcii kybernetických bezpečnostných incidentov. Posledným cieľom práce je navrhnúť a implementovať systém na predikciu kybernetických bezpečnostných incidentov.

Práca je rozdelaná do 5 kapitol. Prvá kapitola predstavuje teoretický úvod do využitia časových údajov v kybernetickej bezpečnosti. V druhej kapitole diskutujeme existujúce prístupy na predikciu kybernetických incidentov. V tretej kapitole rozoberáme spôsoby analýzy kybernetických incidentov vo forme kvantitatívnych časových radov. Štvrtá kapitola sa zaoberá výberom a spacovaním dát s využitím nášho systému na predikciu kvantity kybernetických útokov. Napokon v piatej kapitole sa venujeme návrhu a implementácii používateľskej aplikácie.

Kapitola 1

Analýza časového hľadiska v bezpečnosti

Kybernetická bezpečnosť

Kybernetická bezpečnosť sa vo všeobecnosti zaoberá ochranou aktív nachádzajúcich sa v kybernetickom priestore. Jej cieľom je dodržanie dôvernosti, dostupnosti a integrity týchto aktív [1]. Kybernetická bezpečnosť sa zvyčajne týka počítačov a podobných výpočtových zariadení a ich počítačových sietí. Kybernetická bezpečnosť v oblasti kyberpriestoru sa vyznačuje vysokou náročnosťou správneho naprogramovania, nastavenia a návrhu týchto systémov.

So zvyšujúcou sa mierou digitalizácie sa kyberpriestor zväčšuje, čo v kombinácii s náročnosťou zabezpečenia kyberpriestoru zvyšuje dopyt po kyberbezpečnostných praktikách, postupoch, algoritmoch, ktoré by účinne zabezpečili jeho používateľov a ich dáta.

Kybernetický útok

Útok je akýkoľvek pokus odhaliť, pozmeniť, odstaviť, zničiť, ukradnúť alebo získať neautorizovaný prístup k alebo neautorizovane použiť aktívum [2]. Kybernetický útok je akýkoľvek typ útočného manévra, ktorý má za cieľ narušiť integritu, dostupnosť alebo dôvernosť počítačových informačných systémov, infraštruktúry, počítačových sietí alebo osobných počítačových zariadení. Útočníkom je osoba alebo proces, ktorý sa pokúša získať prístup k dátam, funkciám alebo iným obmedzeným častiam systému bez autorizácie, potenciálne so zákerným úmyslom [3]. V závislosti na kontexte, kybernetické útoky môžu byť súčasťou kybernetickej vojny alebo kybernetického ter-

rorizmu. Kybernetický útok môže byť spôsobeným štátmi, jednotlivcami, skupinami, spoločnosťou alebo organizáciami. Na druhej strane, kybernetický útok môže pochádzať z anonymného zdroja [4].

Kybernetický útok môže ukradnúť, pozmeniť alebo zničiť konkrétny cieľ hacknutím do zraniteľného systému [5]. Kybernetické útoky môžu siahať od inštalovania spywéru na osobný počítač až po pokus o zničenie infraštruktúry celých národov [6]. Kybernetické útoky sa v súčasnej dobe stávajú čoraz sofistikovanejšími a nebezpečnejšími [7]. Behaviorálna analýza používateľov a použitie SIEM systémov pomáha zabrániť týmto útokom [4].

Softvérová chyba

Softvérová chyba predstavuje taký typ chyby, nedostatku alebo zlyhania v počítačovom programe alebo v informačnom systéme, ktoré spôsobuje vyprodukovanie nesprávneho alebo neočakávaného výsledku alebo neúmyselné správanie. Proces hľadania a opravovania týchto chýb sa nazýva „debugovanie“ a často používa formálne techniky alebo nástroje na ohraničenie chýb. Od 50-tych rokov niektoré počítačové systémy boli navrhnuté tak, aby znižovali, detegovali alebo automaticky opravili rôzne počítačové chyby v priebehu ich prevádzky.

Väčšina chýb vzniká v zdrojovom kóde alebo dizajne programu alebo v jeho komponentoch a operačných systémoch používaných programami. Malé množstvo je tvorené kompilátormi produkujúcimi nesprávny kód. Program, ktorý obsahuje veľké množstvo bugov alebo bugy, ktoré zásadne zasahujú do jeho funkcionality, sa nazýva zabugovaný. Bugy môžu spustiť chyby, ktoré majú kaskádové dôsledky. Bugy môžu mať malé vplyvy, ale môžu spôsobiť aj spadnutie programu alebo zaseknúť celý počítač. Iné bugy sa klasifikujú ako bezpečnostné chyby a môžu napríklad dovoliť zlomyseľnému používateľovi obísť kontroly oprávnení za účelom získať neautorizované oprávnenia [8].

Časové rady

Udalosti odohrávajúce sa v jeden moment často súvisia s inými udalosťami odohrávajúcimi v iných momentoch. Môžeme neporozumieť účinkom verejnej alebo internej legislatívy, alebo priebehu fyzických, chemických alebo biologických mechanizmov, ak nepoznáme pôsobenie času vo vzťahoch medzi časovo usporiadanými premennými. Naša schopnosť predpovedať časovo usporiadané premenné môže byť znížená, ak ne-

poznáme časovú štruktúru vzťahov medzi premennými.

Študovanie takýchto vzájomných vzťahov pomocou časovo usporiadaných dát sa volá analýza časových radov. Cieľom v analýze časových vzťahov je nájdenie užitočného spôsobu (modelu) na vyjadrenie časovo štruktúrovaných vzťahov medzi nejakými premennými alebo udalosťami. Potom môžeme tieto vzťahy vyhodnocovať alebo môžeme predpovedať jednu alebo viacero premenných [9].

Využitie času

Čas sa v informačných systémoch využíva v podobe časových pečiatok. Tieto pečiatky sa používajú na označenie času odohratia nejakej udalosti. Informačné systémy môžu vytvárať záznamy o ich činnosti. Tieto záznamy sa používajú na kontrolu a zisťovanie nezvyčajných udalostí.

Z hľadiska bezpečnosti je dôležité mať schopnosť overiť presný čas resp. overiť existenciu dát pred určitým bodom v čase. Toto sa dá docieliť použitím časovej pečiatky od certifikačnej autority [10].

Kapitola 2

Existujúce prístupy

2.1 Podobné práce

V súčasnej dobe existuje niekoľko metód na predikciu kybernetických útokov na základe odpozorovaných javov pozostávajúcich z minulých útokov, prípadne aj iných zdrojov. Kvôli rôznorodosti týchto metód sme ich porovnali pomocou troch nami vybratých základných kategórií: predmet predikcie, použitý model a použité dáta (dataset).

IFS - Intrusion Forecasting System Based on Collaborative Architecture

V tejto práci sa autori snažili ukázať kolaboratívnu architektúru IDS (intrusion detection systems - systémov detegcie prieniku) využívajúcu predikčné prístupy za účelom pokryť nedostatky existujúcich prístupov. Autori rozdelili IDS do troch generácií podľa funkcií: identifikácia a detegcia, prevencia a blokovanie, predikcia a predpoveď. Autorom sa podarilo predpovedať počty UIT (unwanted internet traffic - nevyžiadaná internetová premávka). Autori navrhujú použitie takéhoto systému ako systém skorého varovania [11].

A Neuro-genetic ensemble Short Term Forecasting Framework for Anomaly Intrusion Prediction

V tejto práci autori prezentovali framework pre štatistickú predikciu anomálií využivajúc neurónovú sieť trénovanú genetickým algoritmom. Autori implementovali systém na detegciu budúcich prienikov, ktorý otestovali na datasete MIT Lincoln Labs. Autori došli k záveru, že neuro-genetická predikčná technika prekonáva techniku backpropagation [12].

Real Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Model

V tejto práci autori navrhli framework na predikciu viackrokových útokov. Autori využili Skryté Markovove Modely na modelovanie vzťahov medzi útočníkmi a sieťami. Autori využili koreláciu medzi výstrahami na zníženie počtu falošných negatív v predikcii. Autori ukázali, že ich systém vie perfektne predikovať DDoS útoky na datasete DARPA 2000 [13].

Advanced probabilistic approach for network intrusion forecasting and detection

V tejto práci autori navrhujú probabilistický prístup k predpovedi a detegcii sieťových prienikov. Tento prístup využíva Markovov reťazec pre pravdepodobnostné modelovanie abnormálnych udalostí v sieťovom systéme. Autori ich prístup vyhodnotili pomocou datasetu DARPA 2000. Autori očakávajú, že ich prístup bude integrovaný do existujúcich sieťových IDS, čo by podľa nich malo zapríčiniť skoršiu detegciu útokov [14].

Time Series Forecasting of Cyber Attack Intensity

V tejto práci sa autori pokúsili využiť temporálne korelácie medzi počtami útokov za deň v priebehu viacerých za sebou idúcich dní. Autori predstavujú systém na predikciu počtu kybernetických útokov využívajúc len historické dáta o počtoch útokov. Autori použili ARIMA model na datasete Hackmageddon. Autori došli k záveru, že použitie počtov útokov za deň ako časového radu ukázalo silnú temporálnu koreláciu [15].

Predicting Cyber Attacks With Bayesian Networks Using Unconventional Signals

V tejto práci sa autori zamerali na použitie Bayesovského klasifikátora na klasifikáciu globálnych udalostí za účelom predikcie kybernetických útokov. Autori využili udalosti z datasetov Twitter, GDELT a Hackmageddon [16].

Quickprop Neural Network Short-Term Forecasting Framework for a Database Intrusion Prediction System

V tejto práci autori predstavujú systém na štatistickú predikciu anomálií pomocou Multi-Agentov. Autori vytvorili model na predpovedanie neoprávnených prístupov do

databázy pomocou neurónovej siete. Autori svoj systém vyhodnotili pomocou metriky MAPE s použitím datasetu z nemenovanej veľkej komerčnej banky [17].

Fibonacci Sequence and EWMA for Intrusion Forecasting System

V tejto práci autori skúmali použiteľnosť kooperatívnej architektúry na predpovedanie UIT na hostoch geograficky oddelených. Autori použili kombináciu EWMA a Fibonacciho techniku predpovede [18].

Forecast techniques for predicting increase or decrease of attacks using Bayesian Inference

V tejto práci autori predstavujú techniku predikcie množstva útokov pomocou Bayezovskej Inferencie. Táto technika je použitá na predpovedanie zvýšenia alebo zníženia počtu útokov. Autori vyhodnotili túto techniku pomocou reálnych záznamov z IDS [19].

DIDFAST.BN: Distributed Intrusion Detection And Forecasting Multiagent System using Bayesian Network

V tejto práci autori predstavujú systém na distribuovanú detegciu prienikov a predpoveď multiagentových systémov pomocou Bayesovských sietí. Tento systém sa skladá z dvoch vrstiev: prvá má za úlohu detegciu anomálií a druhá predikciu prienikov založenú na detegciách z prvej vrstvy [20].

A High-efficiency Intrusion Prediction Technology Based on Markov Chain

V tejto práci autori predstavujú techniku na predikovanie prienikov založenú na Markovovom reťazci. Táto technika je veľmi efektívna umožnujúc efektívne spracovanie sieťovej premávky v reálnom čase [21].

IDS 3G - Third Generation for Intrusion Detection: Applying Forecasts and Return on Security Investment to Cope with Unwanted Traffic

V tejto práci autori predstavujú metodológiu na predpovedanie UIT na základe trendov pomocou modelov založených na kĺzavých priemeroch a Fibonacciho postupnosti. Autori na vyhodnotenie využili datasety DARPA a KDD [22].

Práca	Predmet predikcie	Použitý model	Použitý dataset
[11]	Unwanted Internet Traffic (UIT)	SMA + EWMA + Combined SMA + Combined EWMA + Fibonacci sequence	Generované dáta: DoS, R2L, U2R, Scanning
[12]	Sieťové prieniky	Neural Network	KDD, DARPA 2000
[13]	Sieťové prieniky	Hidden Markov Model	MIT Lincoln Laboratory, DARPA 2000
[14]	Sieťové prieniky	APAN (K-means state definition with Markov chain transitions)	DARPA 2000
[15]	Počet útokov	Autoregressive integrated moving average (ARIMA)	Hackmageddon database (2016)
[16]	Kybernetické útoky	Bayesian classifier	Twitter Attack Mentions, GDELT Event Mentions, GDELT Event Tone, Hackmageddon
[17]	Prieniky databázií	Quickprop Neural Network	Data from major Corporate Bank
[18]	UIT (DoS, R2L, U2R, probe)	Fibonacci sequence, EWMA	DARPA 2000
[19]	Počty udalostí IDS	Bayesian Inference: week cycle + fluctuation range	
[20]	Sieťové prieniky	Bayesian Networks	DARPA 2000
[21]	Prieniky	Markov chain + improved FAR, FNR	
[22]	Trendy UIT za krátku dobu (hodiny)	MA (Moving Average), Fibonacci sequence	DARPA 2000, KDD

Tabuľka 2.1: Porovnanie pomocou vybraných hlavných parametrov aktuálnych prístupov k predikcii kybernetických útokov

Z tabuľky 2.1 možno vidieť, že spektrum použitých modelov je z pohľadu zložitosti široké. Toto vidieť aj z faktu, že medzi použitými modelmi sa nachádzajú aj pomerne jednoduchšie modely založené na kĺzavom priemere a taktiež aj zložitejšie modely založené na neurónových sieťach. Taktiež z tabuľky 2.1 vidieť, že použité modely nie sú všetky z jednej oblasti, ale z viacerých. Vysoká rôznorodosť použitých modelov naznačuje, že problém predikcie kybernetických útokov je téma ešte nie bohato preskúmaná. Tabuľka 2.2 bližšie znázorňuje rozdelenie modelov podľa hlavnej oblasti.

Prístup	Práce
Autoregresia	[11], [15], [18], [22]
Markovov reťazec	[13], [14], [21]
Bayesovský pravdepodobnostný	[16], [19], [20]
Neurónová sieť	[12], [17]

Tabuľka 2.2: Porovnanie metód na základe prístupu

Kapitola 3

Analýza bezpečnostných údajov z časového hľadiska

3.1 Metódy a modely predikcie

Metóda predpovedania je algoritmus, ktorý poskytuje bodovú predpoveď, t.j. jednu hodnotu, ktorá je predikciou hodnoty budúcej časovej periódy. Na druhej strane, štatistický model poskytuje stochastické dáta generujúce proces, ktorý môže byť použitý na vyprodukovanie celého rozdelenia pravdepodobnosti pre budúcu časovú periódu. Bodová predpoveď sa v tomto modeli dá ľahko získať zvolením strednej hodnoty alebo mediánu rozdelenia pravdepodobnosti. Model taktiež dovoľuje výpočet predikčných intervalov s vopred zvolenou hladinou spoľahlivosti [23].

ARIMA

Modely ARIMA predstavujú zovšeobecnenie triedy ARMA modelov, ktoré zakomponovávajú široký rozsah nestacionárnych radov. Tieto modely pomocou konečného počtu diferencovaní zabezpečujú stacionaritu časových radov, čo umožňuje použitie ARMA modelov. ARMA modely sú kombinácia autoregresie (AR) a kĺzavých priemerov (MA - moving average) [24].

ARIMA modely sa označujú ARIMA(p, d, q), kde p je stupeň autoregresie, d je počet diferencovaní a q je stupeň kĺzavých priemerov.

Tento model sa dá vyjadriť pomocou vzorca

$$y_t^{(d)} = c + \sum_{i=1}^{p} \phi_i y_{t-i}^{(d)} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j} + \varepsilon_t$$

kde y je rad diferencovaný d-krát, c je konštanta, p je stupeň autoregresie, ϕ sú koeficienty autoregresie, q je stupeň kĺzavých priemerov, θ sú koeficienty kĺzavých priemerov a ε je odchýlka [25].

Dynamická regresia

Model dynamickej regresie opisuje lineárnu závislosť výstupu k aktuálnym a predchádzajúcim hodnotám jedného alebo viacerých vstupov. Bežne sa predpokladá, že pozorovania rôznych radov sa odohrávajú v pravidelných intervaloch. Kritický predpoklad, že vstupy nie sú ovplyvnené výstupom, platí aj v prípade, keď výstup je ovplyvnený vstupmi. Toto znamená, že sme limitovaní na jednorovnicové modely.

Tieto modely vieme reprezentovať rovnicou

$$y_t = c + \sum_{i=0}^{n} v_i x_{t-i} + N_t$$

kde y je výstup, c je konštanta, v sú koeficienty, x je vstup a N je biely šum [9].

Exponenciálne vyrovnávanie

Exponenciálne vyrovnávanie popisuje triedu modelov. Niektoré z najúspešnejších metód predpovedania sú postavené na princípoch exponenciálneho vyrovnávania.

Existuje množstvo metód, ktoré spadajú do rodiny exponenciálneho vyrovnávania. Vyznačujú sa tým, že predpovede sú váženou kombináciou predchádzajúcich pozorovaní s novšími, ktoré majú relatívne vyššiu váhu v porovnaní so staršími pozorovaniami. Názov „exponenciálne vyrovnávanie“ odráža fakt, že váhy sa znižujú exponenciálne so starnutím pozorovaní.

Tento model možno vyjadriť pomocou rovnice

$$\hat{y}_{t+1} = \alpha y_t + (1 - \alpha)\hat{y}_t$$

kde $0 \leq \alpha \leq 1$ je vyhladzovací parameter, y je časový rad a $\hat{y}$ je predpoveď [23].

Neurónové siete

Umelé neurónové siete sú metódy predpovede, ktoré sú založené na jednoduchých matematických modeloch mozgu. Umožňujú modelovať komplikované nelineárne vzťahy medzi závislými premennými a ich prediktormi.

Neurónová sieť môže byť vnímaná ako sieť „neurónov“, ktoré sú usporiadané vo vrstvách. Prediktory (alebo vstupy) tvoria spodnú vrstvu a predpovede (alebo výstupy) tvoria vrchnú vrstvu. Môže existovať aj mnoho medzivrstiev obsahujúcich „skryté“ neuróny.

Najjednoduchšie neurónové siete neobsahujú žiadne skryté vrstvy a sú ekvivalentné lineárnej regresii. Príkladom takejto jednoduchej siete by bola sieť so štyrmi vstupnými neurónmi (prediktormi) a jedným výstupným neurónom. Koeficienty pripojené k týmto prediktorom sa volajú „váhy“. Predpovede sú získavané lineárnou kombináciou vstupov. Váhy siete sa získavajú pomocou „učiaceho algoritmu“, ktorý minimalizuje „chybovú funkciu“ ako napríklad MSE (mean squared error - priemer štvorcov odchyliek) [25].

3.2 Ohodnotenie miery presnosti predikcie

Na meranie presnosti predpovede existuje viacero spôsobov. V tejto práci sme sa zamerali na tie, ktoré využívajú odchýlku medzi predikciami a pozorovanými hodnotami. Zadefinujeme odchýlku (error) ako

$$\varepsilon_t = y_t - \hat{y}_t$$

kde y je pozorovaná hodnota a $\hat{y}$ je predpoveď [26].

Miery závislé na mierke

Niektoré z najpoužívanejších mier sú miery, ktorých hodnota je závislá od mierky dát. Tieto miery sú užitočné pri porovnávaní metód na tých istých dátach, avšak nemali by sa používať pri porovnávaní s dátami s rozdielnymi mierkami.

$$\begin{aligned} \text{Mean Square Error (MSE)} &= \text{priemer}(\varepsilon_t^2) \\ \text{Root Mean Square Error (RMSE)} &= \sqrt{\text{MSE}} \\ \text{Mean Absolute Error (MAE)} &= \text{priemer}(|\varepsilon_t|) \\ \text{(MdAE)} &= \text{medián}(|\varepsilon_t|) \end{aligned}$$

[26]

Percentuálne miery

Tieto miery k svojmu výpočtu využívajú percentuálnu odchýlku. Tú zadefinujeme ako $p_t = 100\varepsilon_t/y_t$. Tieto miery majú ako výhodu to, že sú nezávislé na mierke dát,

avšak majú zase tú nevýhodu, že si nevedia poradiť s prípadmi keď dáta majú nulové hodnoty alebo hodnoty blízke nule.

$$\begin{aligned} \text{Mean Absolute Percentage Error (MAPE)} &= \text{priemer}(|p_t|) \\ \text{Median Absolute Percentage Error (MdAPE)} &= \text{medián}(|p_t|) \\ \text{Root Mean Square Percentage Error (RMSPE)} &= \sqrt{\text{priemer}(p_t^2)} \\ \text{Root Median Square Percentage Error (RMdSPE)} &= \sqrt{\text{medián}(p_t^2)} \end{aligned}$$

[26]

Škálované miery

Škálované miery sú postavené na relatívnych odchýlkach s cieľom odstrániť škálu dát. Zadefinujeme vyškálovanú odchýlku ako

$$q_t = \frac{\varepsilon_t}{\frac{1}{n-1}\sum_{i=2}^{n}|y_i - y_{i-1}|}$$

kde ε je odchýlka, y je pozorovaná hodnota a n je dĺžka radu.

$$\text{Mean Absolute Scaled Error (MASE)} = \text{priemer}(|q_t|)$$

[26]

Kapitola 4

Spracovanie bezpečnostných údajov

4.1 Príprava dát

Pri návrhu riešenia sme pracovali s datasetom, ktorý pochádza zo systému WARDEN od skupiny CESNET. Sú to záznamy z rôznych sieťových sond, honeypotov. Tieto záznamy sa nachádzajú vo formáte IDEA, ktorý bol vyvinutý skupinou CESNET. Uvedený formát sa používa na zjednotenie záznamov z veľkého množstva rôzneho software. Každý záznam obsahuje zopár povinných parametrov a viacero nepovinných. V našej práci sme využili len parametre Timestamp, Category, Port, Protocol.

Pre naše záznamy sme najprv vytiahli údaje s požadovanými stĺpcami z databázy do súboru vo formáte csv. Tento súbor sme potom importovali do programovacieho prostredia RStudio [27] bežiacom na školskom serveri, ktoré nám umožnilo spracovanie v programovacom jazyku R [28]. Importovali sme ho pomocou funkcie `read_delim` z balíka *readr* [29], ktorá nám vytvorila objekt typu `data.frame` so 4 znakovými stĺpcami a 295538507 riadkami. Najprv sme nahradili bunky, ktoré neobsahovali žiadnu hodnotu (indikovanú reťazcami `"NO VALUE"`) natívnym R typom `NA`. Záznami sme ďalej transformovali pomocou funkcií `transmute` z balíka *tibble* [30] a vlastnej funkcie zo znakového reťazca na vyššiu dátovú štruktúru `list`. Toto nám potom umožnilo vyfiltrovať záznamy určené len na testovanie - toto boli záznamy, ktoré obsahujú len kategóriu `"Test"`. Výsledkom bolo 295530112 použiteľných záznamov.

Na takto upravenom datasete sme potom vygenerovali štatistiky vyskytujúcich sa kategórií, protokolov a skombinovaných tcp a udp portov.

Kategória	Počet záznamov	Percento datasetu
Recon.Scanning	248475373	84.078%
Test	53101809	17.968%
Attempt.Login	26533433	8.978%
Attempt.Exploit	12845238	4.347%
Malware.Ransomware	3191557	1.080%
Intrusion.Botnet	1799159	0.609%
Abusive.Spam	899921	0.305%
Availability.DoS	743115	0.251%
Information.UnauthorizedAccess	678288	0.230%
Suspicious.TOR	165795	0.056%

Tabuľka 4.1: Počty záznamov pre top 10 kategórií

Každý záznam bol označený jednou alebo viacerými kategóriami. Z datasetu bolo potrebné vyfiltrovať len tie záznamy, ktoré boli označené iba kategóriou Test.

Protokol	Počet záznamov	Percento datasetu
tcp	170164003	57.579%
ssh	15396932	5.210%
udp	10882153	3.682%
icmp	9862729	3.337%
ms-wbt-server	5716384	1.934%
telnet	4311724	1.459%
dns	429164	0.145%
sip	266482	0.090%
ip	182868	0.062%
http	79061	0.027%

Tabuľka 4.2: Počty záznamov pre top 10 protokolov

Port	Počet záznamov	Percento datasetu
23	51767429	17.517%
445	45438778	15.375%
22	25811900	8.734%
80	8465889	2.865%
81	4838845	1.637%
82	2754028	0.932%
443	845086	0.286%
21	754029	0.255%
25	450881	0.153%
88	348362	0.118%

Tabuľka 4.3: Počty záznamov z celého datasetu pre top 10 vybraných portov

Pre porty sme kvôli veľkému objemu dát urobili štatistiky len pre prvých 100000 záznamov a pomocou nich sme sa rozhodli vytvoriť štatistiky len pre vybrané porty na celom datasete.

4.2 Spracovanie dát

Tvorba časových radov

Pomocou týchto štatistík sme sa rozhodli orientovať len na kategórie Recon.Scanning, Attempt.Login, Attempt.Exploit, Malware.Ransomware a Intrusion.Botnet. Z portov sme vybrali porty 23, 445, 22, 80, 81, 443, 21 a 25. Z protokolov sme vybrali tcp, ssh, udp, icmp, ms-wbt-server a telnet.

Pre každý takýto výber sme potom vytvorili dva jednohodnotové časové rady s veľkosťami intervalov deň a hodina s periódami 7 a 24. Takéto časové rady sme vygenerovali ako počet záznamov vyskytujúcich sa v danom intervale.

Funkcia `window` z balíčka *forecast* [31] nám potom dovolila vytvoriť nový časový rad ako časový výsek z radu.

Tieto časové rady sme potom použili ako vstupné dáta pre nami vybrané metódy.

Aplikácia predikčných metód

Na týchto jednotných radoch sme aplikovali nami vybrané metódy.

Vybrali sme štyri metódy, ktoré predstavujú klasické, dobré známe metódy, ale aj novšie, pomerne málo preskúmané. Rozhodli sme sa použiť metódy ARIMA, Dynamická regresia, Exponenciálne vyrovnávanie a Neurónové siete.

Pomocou hotových balíčkov v jazyku R sme aplikovali modely našich metód na našich radoch. Pre metódu ARIMA bola použitá R funkcia `auto.arima` z balíčka *forecast*, ktorá automaticky vyberie najlepšie parametre pre veľkosť autoregresie, kĺzavých priemerov a stupňa diferencie tak, aby rad spĺňal podmienku stacionarity. Pre neurónovú sieť bolo použitých 10 neurónov v 1 skrytej vrstve. Dynamická harmonická regresia použila furierovú aproximáciu s 3 členmi.

Pomocou týchto modelov sme vytvorili predikcie našich dát. Niektoré metódy dávajú len bodové predikcie, iné poskytujú predikčné intervaly. Z predikčných intervalov sme vytvorili bodové predikcie použitím ich stredu.

Ohodnotenie predikcií podľa mier presnosti

Presnosť predikcií modelov sme ohodnotili pomocou miery MASE.

Časové rady sme rozdelili na trénovaciu a testovaciu časť v pomere 80% : 20%. Pre každý časový rad prvá časť predstavovala trénovací interval a hneď po ňom nasledoval testovací interval.

Na trénovacom intervale sme natrénovali modely a tie vytvorili predikcie pre testovací interval. Na testovacom intervale sme porovnali predikcie so skutočnosťou vytvorením odchyliek, ktoré boli spacované pomocou zvolenej metriky, čo nám umožnilo vytvoriť ohodnotenie týchto predikcií.

Výber vhodného modelu

Na základe ohodnotenia predikcií sme určili efektivitu daných modelov pre predikciu nášho datasetu. Pomocou hodnôt vygenerovaných zvolenou mierou sme porovnali jednotlivé metódy navzájom na rovnakých radoch. Na základe získaných údajov sme stanovili poradie efektivity jednotlivých modelov pre predikciu nášho datasetu.

4.3 Dosiahnuté výsledky

V rámci práce sme porovnali štyri metódy pomocou jednotnej miery presnosti na jednotných dátach.

Metóda	Porty	Protokoly	Kategórie	Celkovo
ARIMA	1.48	2.55	1.53	1.85
Exponenciálne vyrovnávanie	1.54	2.58	1.63	1.91
Neurónová sieť	1.70	2.26	1.70	1.89
Dynamická harmonická regresia	1.41	2.03	1.75	1.71

Tabuľka 4.4: Ohodnotenia jednotlivých metód pre rady s intervalom 1 deň a periódou 7.

Metóda	Porty	Protokoly	Kategórie	Celkovo
ARIMA	2.76	2.53	1.48	2.33
Exponenciálne vyrovnávanie	2.78	2.68	1.60	2.42
Neurónová sieť	2.89	3.06	3.64	3.15
Dynamická harmonická regresia	2.63	2.64	1.48	2.34

Tabuľka 4.5: Ohodnotenia jednotlivých metód pre rady s intervalom 1 hodina a periódou 24.

Stĺpce Porty, Protokoly a Kategórie v tabuľke 4.4 predstavujú priemernú hodnotu zo všetkých radov odfiltrovaných (agregovaných) týmto spôsobom. Stĺpec Celkovo

predstavuje priemernú hodnotu zo všetkých radov.

Tabuľky 4.4 a 4.5 zachytávajú presnosti jednotlivých metód podľa miery MASE. Hodnota tejto miery je založená na odchýlke medzi predpovedanou hodnotou a skutočnou, nameranou hodnotou. Teda ideálna, perfektná metóda by mala hodnotu 0.

Z porovnania získaných údajov v tabuľke 4.4 vyplýva, že celkovo najlepšou metódou na predpoveď denných hodnôt je Dynamická harmonická regresia.

Na druhej strane, z porovnania získaných údajov v tabuľke 4.5 vyplýva, že celkovo najlepšou metódou na predpoveď hodinových hodnôt je ARIMA.

Kapitola 5

Návrh a implementácia aplikácie

Aplikáciu sme sa rozhodli implementovať pomocou technológie R Shiny [32]. Túto technológiu sme vybrali pretože je implementovaná v programovacom jazyku R, takisto ako balíčky a funkcie použité na prípravu a analýzu datasetu. Táto technológia nám umožnila vytvoriť interaktívnu webovú aplikáciu bez nutnosti použiť viacero odlišných programovacích jazykov a pracovať len v jazyku R, čo bolo pre nás veľkou výhodou.

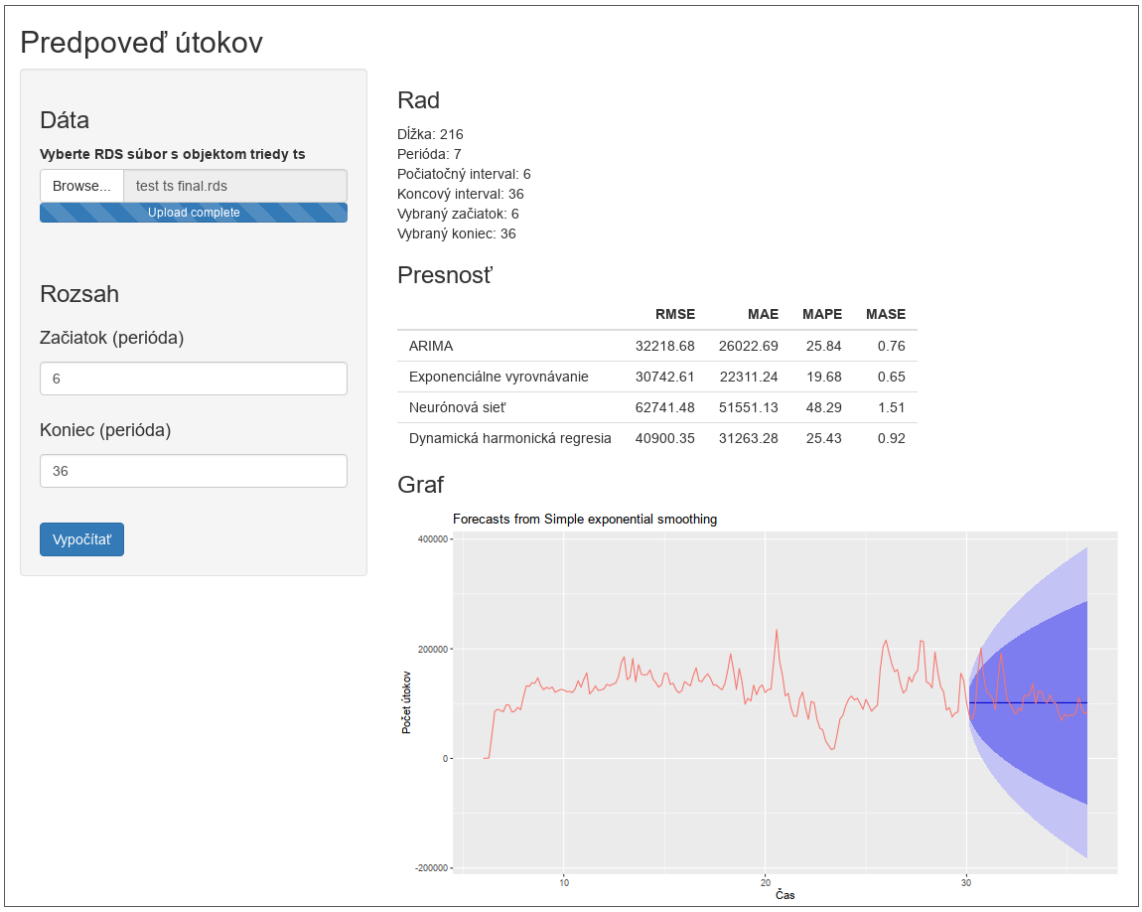
Aplikácie Shiny sa skladajú z dvoch častí: používateľskej a serverovej. V používateľskej časti je definované používateľské prostredie, ktoré sa zobrazí používateľovi aplikácie po jej spustení. V serverovej časti je definované správanie aplikácie vrátane výpočtov a obsluhy používateľského prostredia [33].

Naša aplikácia umožňuje nahrať súbor s časovým radom a na ňom spustiť naše vybrané metódy. Aplikácia umožňuje použiť celý rad alebo vybrať len úsek radu na analýzu. Vybraný úsek je potom automaticky rozdelený na trénovaciu a testovaciu časť a na týchto častiach sú natrénované a ohodnotené jednotlivé predikčné metódy, tak ako to je popísané v sekcii 4.2. Hodnotenie týchto modelov je potom zobrazené v tabuľke. Pre model s najlepším ohodnotením je potom vygenerovaný graf.

```
model_arima      = auto.arima(okno_trening, seasonal = TRUE);
predpoved_arima = forecast(model_arima, h = (b - b2) * f);
presnost_arima  = accuracy(f = predpoved_arima, x = rad);

predpoved = predpoved_arima;
presnost  = presnost_arima[2, 6];

predpoved_ses = ses(okno_trening, h = (b - b2) * f);
presnost_ses  = accuracy(f = predpoved_ses, x = rad);

if(presnost_ses[2, 6] < presnost) {
        predpoved = predpoved_ses;
        presnost  = presnost_ses[2, 6];
}

model_nn      = nnetar(okno_trening, p = f, size = 10);
predpoved_nn = forecast(model_nn, h = (b - b2) * f);
presnost_nn  = accuracy(f = predpoved_nn, x = rad);

if(presnost_nn[2, 6] < presnost) {
        predpoved = predpoved_nn;
        presnost  = presnost_nn[2, 6];
}

reg           = fourier(okno_trening, K = 3);
model_dhr     = auto.arima(okno_trening, xreg = reg,
seasonal = FALSE, lambda = 0);
reg           = fourier(okno_trening, K = 3, h = (b - b2) * f);
predpoved_dhr = forecast(model_dhr, xreg = reg);
presnost_dhr  = accuracy(f = predpoved_dhr, x = rad);

if(presnost_dhr[2, 6] < presnost) {
        predpoved = predpoved_dhr;
}
```

Ukážka kódu na výpočet a výber modelov

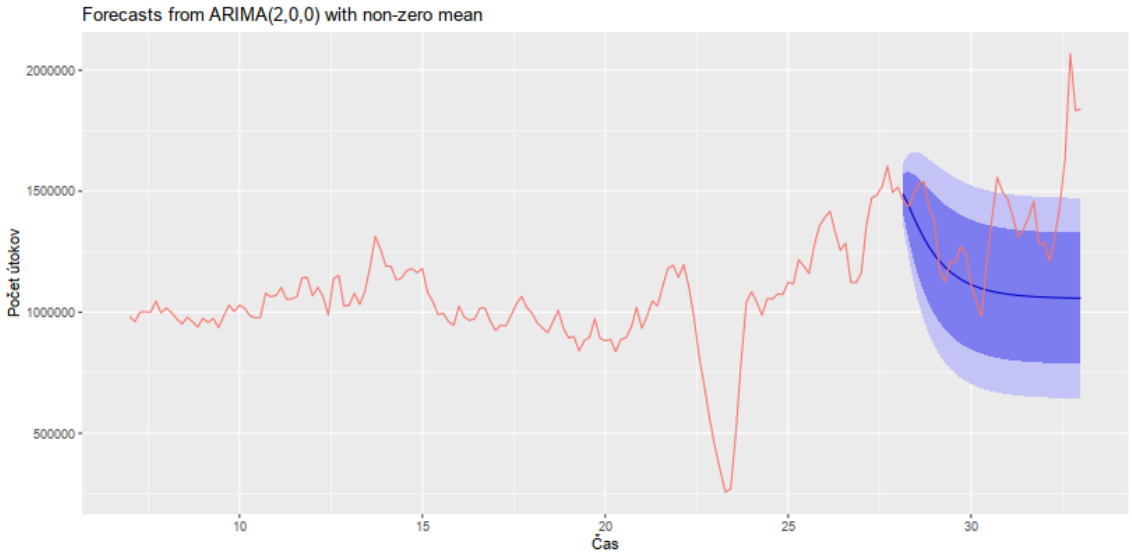
Ukážka kódu zobrazuje, že aplikácia postupne vytvára modely, ich predikcie a ich ohodnotenia pre každú metódu, pričom si pamätá metódu s najlepšou presnosťou.



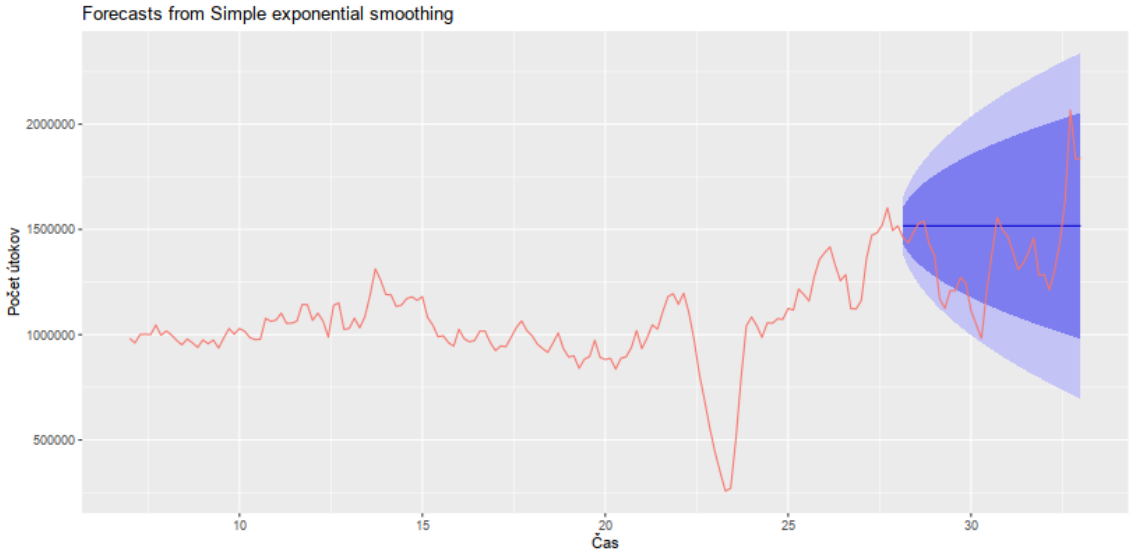
Obr. 5.1: Ukážka aplikácie

Nasledujúce obrázky zobrazujú predikcie štyroch rôznych modelov na rovnakom časovom rade. Z nich možno vidieť, že rozdielne metódy môžu produkovať odlišné predikcie.

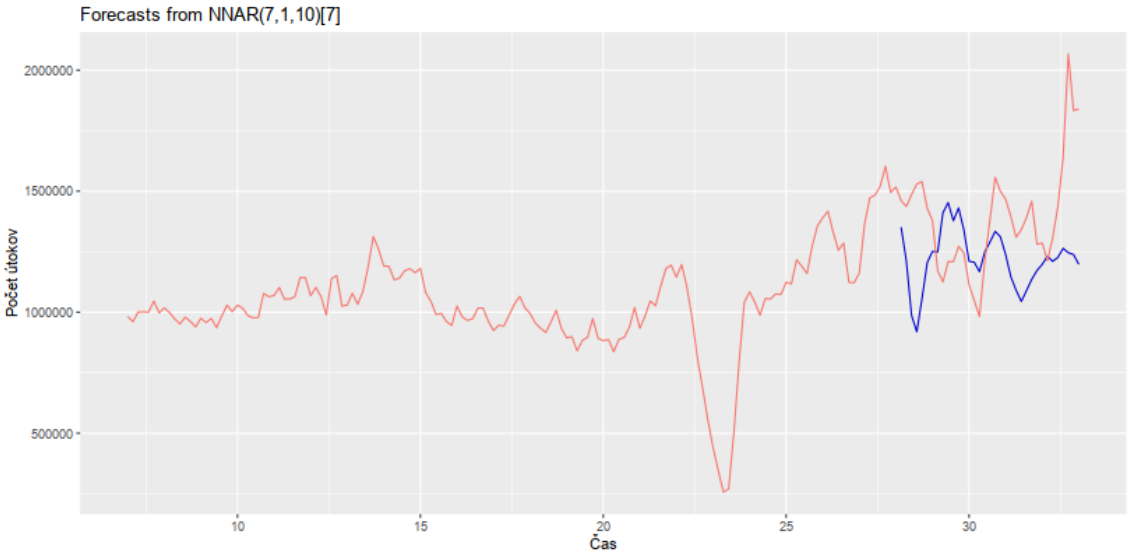
Na obrázkoch 5.2 až 5.5 sú graficky zobrazené predpovede jednotlivých modelov voči skutočným údajom časového radu. Červenou farbou sú znázornené hodnoty časového radu. Modrou farbou sú znázornené predikčné intervaly modelu. Pri absolútnej presnosti by predikcia modelu zakreslená modrou čiarou úplne kopírovala hodnoty radu zakreslené červenou čiarou.



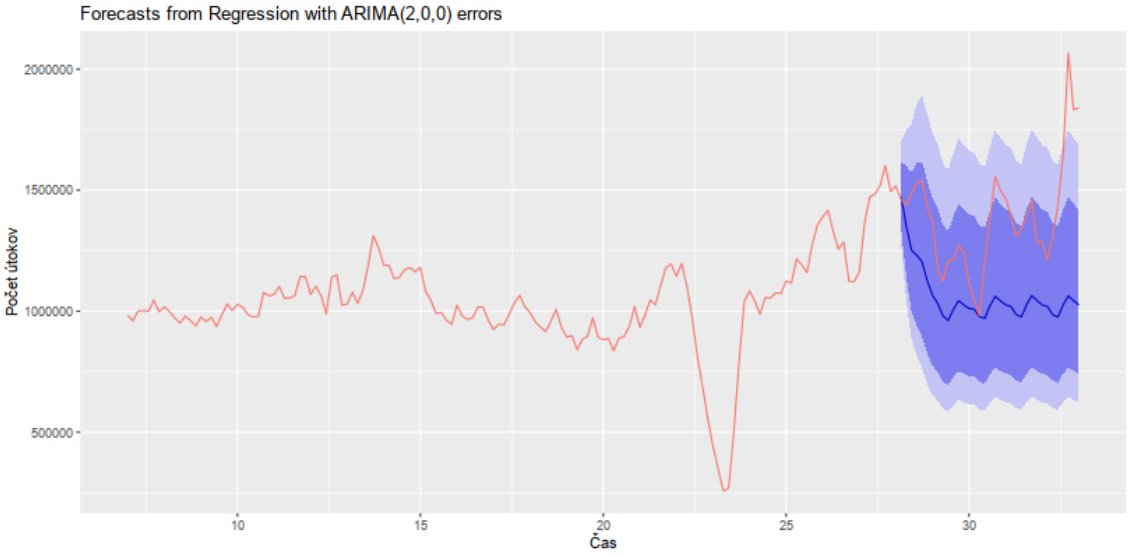
Obr. 5.2: Predpoveď modelu ARIMA pre časový rad kategórie Recon.Scanning a interval 1 deň



Obr. 5.3: Predpoveď modelu Exponenciálne vyrovnávanie pre časový rad kategórie Recon.Scanning a interval 1 deň



Obr. 5.4: Predpoveď modelu Neurónová sieť pre časový rad kategórie Recon.Scanning a interval 1 deň



Obr. 5.5: Predpoveď modelu Dynamická harmonická regresia pre časový rad kategórie Recon.Scanning a interval 1 deň

Záver

Táto záverečná práca sa venovala použitiu času v rámci kybernetickej a aj informačnej bezpečnosti. Ako sme aj v práci poukázali, časová pečiatka predstavuje neoddeliteľnú súčasť všetkých bezpečnostných údajov. Slúži na presné určenie časovej následnosti jednotlivých bezpečnostných udalostí.

V rámci záverečnej práce sme si stanovili tri ciele. Prvým cieľom bola analýza štatistických metód použitých na predikciu bezpečnostných udalostí použitím časového hľadiska bezpečnostných udalostí. Tomuto cieľu sa venujeme v tretej kapitole tejto práce. Rozoberáme niekoľko metód predikcie, medzi ktoré môžeme zaradiť ARIMA modely, model dynamickej regresie, exponenciálne vyhladzovanie, resp. aj všeobecné metódy ako neurónové siete. Súčasťou analýzy týchto metód je aj diskusia ohľadne mier použitých pre určenie presnosti predikcie. V rámci kapitoly sa zameriavame na miery, ktoré využívajú odchýlku medzi predikciami a pozorovanými hodnotami (napr. Mean Square Error, Mean Absolute Error, Median Absolute Error).

Druhým cieľom práce bola analýza a porovnanie aktuálnych prístupov k predikcii kybernetických bezpečnostných udalostí. Tomuto cieľu je venovaná druhá kapitola tejto záverečnej práce. Podľa vybraných parametrov (predmet predikcie, použitý model a použité údaje k predikcii) sme porovnali 12 vedeckých článkov.

Posledným cieľom tejto záverečnej práce bolo navrhnúť a implementovať systém na predikciu kybernetických bezpečnostných udalostí. Tomuto cieľu sa venujeme v piatej kapitole.

Prácu je možné rozšíriť o analýzu viacerých časových radov. Doplnenie o časové rady vyjadrujúce vývoj bezpečnostných hrozieb v čase by mohol v kombinácii s časovými radmi bezpečnostnými udalosťami napomôcť pri identifikácii zero day (zero hour) zraniteľností.

Zoznam použitej literatúry

[1] *ISO/IEC 27032:2012: Information technology - Security techniques - Guidelines for cybersecurity.* International Organization for Standardization, Geneva, Switzerland.

[2] *ISO/IEC 27000:2009: Information technology - Security techniques - Information security management systems - Overview and vocabulary.* International Organization for Standardization, Geneva, Switzerland. Dostupné na: `http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip`

[3] *ISTQB: Standard glossary of terms used in Software Testing.* [cit. 26. 6. 2019] Dostupné na: `http://glossar.german-testing-board.info/`

[4] *Wikipedia: Cyberattack* [online], [cit. 26. 6. 2019] Dostupné na: `https://en.wikipedia.org/wiki/Cyberattack`

[5] Tom C. W. Lin et al., 2016. Financial Weapons of War. In: *Minnesota Law Review, Vol. 100, p. 1377, 2016; Temple University Legal Studies Research Paper No. 2016-25.*

[6] Raphael Satter, 2017. What makes a cyberattack? Experts lobby to restrict the term [online]. [cit. 26. 6. 2019] Dostupné na: `https://apnews.com/2c25d7da76f4409bae7daf063c071420`

[7] Stamatis Karnouskos, 2011. Stuxnet worm impact on industrial cyber-physical system security. In: *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2011. p. 4490-4494.*

[8] *Wikipedia: Software bug* [online], [cit. 26. 6. 2019] Dostupné na: `https://en.wikipedia.org/wiki/Software_bug`

[9] Alan Pankratz, 1991. *Forecasting with Dynamic Regression Models.* United States of America: John Wiley & Sons, Inc. ISBN 0-471-61528-5

[10] C. Adams et al., 2001. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*

[11] Elvis Pontes et al., 2009. IFS-Intrusion forecasting system based on collaborative architecture. In: *Digital Information Management, 2009. ICDIM 2009. Fourth International Conference on. IEEE, 2009.*

[12] Siva S.Sivatha Sindhu et al., 2006. A neuro-genetic ensemble short term forecasting framework for anomaly intrusion prediction. In: *Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on. IEEE, 2006.*

[13] Alireza Shameli Sendi et al., 2012. Real time intrusion prediction based on optimized alerts with hidden Markov model. In: *Journal of networks 7.2 (2012): 311.*

[14] Seongjun Shin et al., 2012. Advanced probabilistic approach for network intrusion forecasting and detection. In: *Expert systems with applications 40.1 (2013): 315-322.*

[15] Gordon Werner et al., 2017. Time series forecasting of cyber attack intensity. In: *Proceedings of the 12th Annual Conference on cyber and information security research. ACM, 2017.*

[16] Ahmet Okutan et al., 2017. Predicting cyber attacks with bayesian networks using unconventional signals. In: *Proceedings of the 12th Annual Conference on Cyber and Information Security Research. ACM, 2017.*

[17] Ramasubramanian P. et al., 2004. Quickprop neural network ensemble forecasting framework for a database intrusion prediction system. In: *Neural Information Processing-Letters and Reviews 5.1 (2004): 9-18.*

[18] Elvis Pontes et al., 2010. Fibonacci sequence and EWMA for intrusion forecasting system. In: *Digital Information Management (ICDIM), 2010 Fifth International Conference on. IEEE, 2010.*

[19] Chie Ishida et al., 2005. Forecast techniques for predicting increase or decrease of attacks using bayesian inference. In: *Communications, Computers and signal Processing, 2005. PACRIM. 2005 IEEE Pacific Rim Conference on. IEEE, 2005.*

[20] Farah Jemili et al., 2006. DIDFAST.BN: distributed intrusion detection and forecasting multiagent system using Bayesian network. In: *Information and Communication Technologies, 2006. ICTTA'06. 2nd. Vol. 2. IEEE, 2006.*

[21] Cao Lai-Cheng, 2007. A high-efficiency intrusion prediction technology based on markov chain. In: *Computational Intelligence and Security Workshops, 2007. CISW 2007. International Conference on. IEEE, 2007.*

[22] Elvis Pontes et al., 2009. Third generation for intrusion detection: applying forecasts and ROSI to cope with unwanted traffic. In: *Proceedings of 4th IEEE ICITST 9 (2009): 1-6.*

[23] Rob J. Hyndman et al., 2008. *Forecasting with Exponential Smoothing The State Space Approach*. Germany: Springer-Verlag Berlin Heidelberg. ISBN 978-3-540-71916-8

[24] Peter J. Brockwell et al., 2016. *Introduction to Time Series and Forecasting Third Edition*. Switzerland: Springer International Publishing. ISBN 978-3-319-29852-8

[25] Rob J. Hyndman et al., 2018. *Forecasting: principles and practice, 2nd edition*. Australia: OTexts. [cit. 26. 6. 2019] Dostupné na: `https://otexts.com/fpp2/`

[26] Rob J. Hyndman et al., 2005. *Another look at measures of forecast accuracy*. In: *International journal of forecasting, 2006, 22.4: 679-688.*

[27] RStudio Team, 2018. *RStudio: Integrated Development Environment for R*. `http://www.rstudio.com/`

[28] R Core Team, 2019. *R: A Language and Environment for Statistical Computing*. `https://www.R-project.org/`

[29] Hadley Wickham et al., 2018. *readr: Read Rectangular Text Data*. R package version 1.3.1. `https://CRAN.R-project.org/package=readr`

[30] Kirill Müller et al., 2019. *tibble: Simple Data Frames*. R package version 2.1.1. `https://CRAN.R-project.org/package=tibble`

[31] Rob Hyndman et al., 2019. *forecast: Forecasting functions for time series and linear models*. R package version 8.7. `http://pkg.robjhyndman.com/forecast`

[32] Winston Chang et al., 2019. *shiny: Web Application Framework for R*. R package version 1.3.2. https://CRAN.R-project.org/package=shiny

[33] *Shiny: The basic parts of a Shiny app*, [cit. 30. 6. 2019] Dostupné na: http://shiny.rstudio.com/articles/basics.html