Časové hľadisko v kybernetickej bezpečnosti

Radovan Fuska

3Ib, 2018 – 2019

**Abstrakt.** Kybernetická bezpečnosť je vždy aktuálna téma. Kybernetická bezpečnosť a bezpečnosť ako taká je veľmi obšírna téma a jej problematika obsahuje veľké množstvo uhlov pohľadov – spôsobov na jej riešenie. V tejto práci sme sa zamerali a tie spôsoby, ktoré riešia jej časové aspekty. Porovnali a analyzovali sme aktuálne spôsoby predikcie kybernetických útokov.

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

1. **Úvod**

Bezpečnosť je vždy aktuálna téma. Má výrazný vplyv na náš majetok, prácu, živobytie, zasahuje prakticky do každého aspektu našich životov. K jej dosiahnutiu štandardne používame mnoho fyzických, ale aj iných prostriedkov, nástrojov. Napríklad na zabezpečenie nášho domova používame dvere so zámkami na kľúče, ktoré majú len osoby, ktorým sme dovolili prístup, pretože sme usúdili, že pre nás nepredstavujú nebezpečenstvo.

Kybernetická bezpečnosť je časť bezpečnosti, ktorá sa zaoberá kyberpriestorom. Kybernetická bezpečnosť sa zvyčajne týka počítačov a podobných výpočtových zariadení a ich sietí. Kybernetická bezpečnosť je v oblasti kyberpriestoru dobre známa téma hlavne vďaka náročnosti 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.

Dôležitou časťou bezpečnosti je pripravenosť. Pripravenosť je schopnosť vysporiadať sa so situáciou, ktorá ešte nenastala, ale vieme, že môže nastať. Na to, aby sme sa mohli na takúto situáciu pripraviť, musíme si byť v prvom rade vedomý možnosti, že takáto situácia môže nastať. Informácie o existencii a špecifikách takejto situácie štandardne získavame z našich skúseností priamo, tým, že sme takúto situáciu už zažili, alebo o nej počuli, alebo pomocou logických úvah vieme predpokladať existenciu takejto situácie. V tejto práci sme sa zamerali na spracovanie predchádzajúcich skúseností s kybernetickými útokmi a to najmä ich temporálnych vlastností.

Dosiahnuť pripravenosť v kyberpriestore však môže predstavovať problém kvôli vysokej zložitosti kybernetických systémov a vysokej kvantite dát používaných na analýzu týchto systémov. Pri riešení problému kybernetickej bezpečnosti sa často používajú automatizované riešenia ako algoritmy a programy. V tejto práci sme sa zamerali na algoritmy spracovávajúce kybernetické útoky z časového hľadiska.

Medzi naše ciele patrí:

* Analýza štatistických metód využívajúcich časové hľadisko v kybernetickej bezpečnosti
  + porovnanie existujúcich metód predikcie kybernetických útokov
* Porovnanie aktuálnych prístupov k predikcii kybernetických bezpečnostných incidentov
  + vyhodnotenie presnosti predikcie vybratých metód pomocou zvoleného datasetu
* Návrh a implementácia systému na predikciu kybernetických bezpečnostných incidentov
  + vytvorenie a vyhodnotenie novej metódy na základe poznatkov získaných z analýzy existujúcich riešení

1. **Súčasný stav**

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

**Tabuľka 1.** Porovnanie pomocou vybratých hlavných parametrov aktuálnych prístupov k predikcii kybernetických útokov

| Práca | Predmet predikcie | Použitý model | Použitý dataset |
| --- | --- | --- | --- |
| [1] | Unwanted Internet Traffic (UIT) (unproductive and useless + malicious (worm, virus, spam, DoS, DDoS) traffic) | SMA (Simple Moving Averages) + Exponential Weighted Moving Averages (EWMA) + Combined SMA + Combined EWMA + Fibonacci sequence | Generované dáta:  DoS (SYN flood, Ping of Death),  Remote to local (R2L),  User to root (U2R) (buffer overflow, SQL injection),  Probe (scanning) |
| [2] | Network intrusions | Neural Network | KDD (Knowledge Discovery and Data Mining),  DARPA 2000 |
| [3] | Network intrusions | Hidden Markov Model | MIT Lincoln Laboratory,  DARPA 2000 |
| [4] | Network intrusions | APAN (K-means state definition with Markov chain transitions) | DARPA 2000 |
| [5] | Number of attacks | Autoregressive integrated moving average (ARIMA) | Hackmageddon database (2016) |
| [6] | Cyber attacks | Bayesian classifier | Twitter Attack Mentions,  GDELT Event Mentions,  GDELT Event Tone,  Hackmageddon |
| [7] | Database intrusions | Quickprop Neural Network | Data from major Corporate Bank |
| [8] | UIT (DoS, R2L, U2R, probe) | Fibonacci sequence,  EWMA | DARPA 2000 |
| [9] | IDS event counts | Bayesian Inference: week cycle + fluctuation range (increase/decrease) (more/less than double/half than previous term) |  |
| [10] | Network intrusions | Bayesian Networks | DARPA 2000 |
| [11] | Intrusions | Markov chain + improved FAR, FNR |  |
| [12] | UIT incident trends in short term (hours) | MA (Moving Average),  Fibonacci sequence | DARPA 2000,  KDD |

Ako je vidieť z tabuľky 1, použité modely nie sú všetky z jednej oblasti, ale z viacerých. Tabuľka 2 bližšie znázorňuje toto rozdelenie.

**Tabuľka 2.** Porovnanie metód na základe hlavnej oblasti

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Práca | Autoregression | Markov chain | Bayesian probabilistic | Neural network |
| [1] | X |  |  |  |
| [2] |  |  |  | X |
| [3] |  | X |  |  |
| [4] |  | X |  |  |
| [5] | X |  |  |  |
| [6] |  |  | X |  |
| [7] |  |  |  | X |
| [8] | X |  |  |  |
| [9] |  |  | X |  |
| [10] |  |  | X |  |
| [11] |  | X |  |  |
| [12] | X |  |  |  |

1. **Záver**

Porovnali sme aktuálne riešenia problému predikcie. Našimi najbližšími krokmi bude návrh, implementácia a následná analýza nášho systému na predikciu kybernetických útokov.

**Literatúra**

1. Pontes, Elvis, and Adilson E. Guelfi. "IFS—Intrusion forecasting system based on collaborative architecture." Digital Information Management, 2009. ICDIM 2009. Fourth International Conference on. IEEE, 2009.
2. Sindhu, Siva S. Sivatha, et al. "A neuro-genetic ensemble short term forecasting framework for anomaly intrusion prediction." Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on. IEEE, 2006.
3. Sendi, Alireza Shameli, et al. "Real time intrusion prediction based on optimized alerts with hidden Markov model." Journal of networks 7.2 (2012): 311.
4. Shin, Seongjun, et al. "Advanced probabilistic approach for network intrusion forecasting and detection." Expert systems with applications 40.1 (2013): 315-322.
5. Werner, Gordon, Shanchieh Yang, and Katie McConky. "Time series forecasting of cyber attack intensity." Proceedings of the 12th Annual Conference on cyber and information security research. ACM, 2017.
6. Okutan, Ahmet, Shanchieh Jay Yang, and Katie McConky. "Predicting cyber attacks with bayesian networks using unconventional signals." Proceedings of the 12th Annual Conference on Cyber and Information Security Research. ACM, 2017.
7. Ramasubramanian, P., and A. Kannan. "Quickprop neural network ensemble forecasting framework for a database intrusion prediction system." Neural Information Processing-Letters and Reviews 5.1 (2004): 9-18.
8. Pontes, Elvis, and Wagner L. Zucchi. "Fibonacci sequence and EWMA for intrusion forecasting system." Digital Information Management (ICDIM), 2010 Fifth International Conference on. IEEE, 2010.
9. Ishida, Chie, et al. "Forecast techniques for predicting increase or decrease of attacks using bayesian inference." Communications, Computers and signal Processing, 2005. PACRIM. 2005 IEEE Pacific Rim Conference on. IEEE, 2005.
10. Jemili, Farah, Montaceur Zaghdoud, and M. Ben Ahmed. "DIDFAST. BN: distributed intrusion detection and forecasting multiagent system using Bayesian network." Information and Communication Technologies, 2006. ICTTA'06. 2nd. Vol. 2. IEEE, 2006.
11. Lai-Cheng, Cao. "A high-efficiency intrusion prediction technology based on markov chain." Computational Intelligence and Security Workshops, 2007. CISW 2007. International Conference on. IEEE, 2007.
12. Pontes, E., and A. E. Guelfi. "Third generation for intrusion detection: applying forecasts and ROSI to cope with unwanted traffic." Proceedings of 4th IEEE ICITST 9 (2009): 1-6.