SITUAČNÉ POVEDOMIE V KYBERNETICKEJ BEZPEČNOSTI

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Situačné povedomie

Situačné povedomie (Situational Awareness, **SA**)

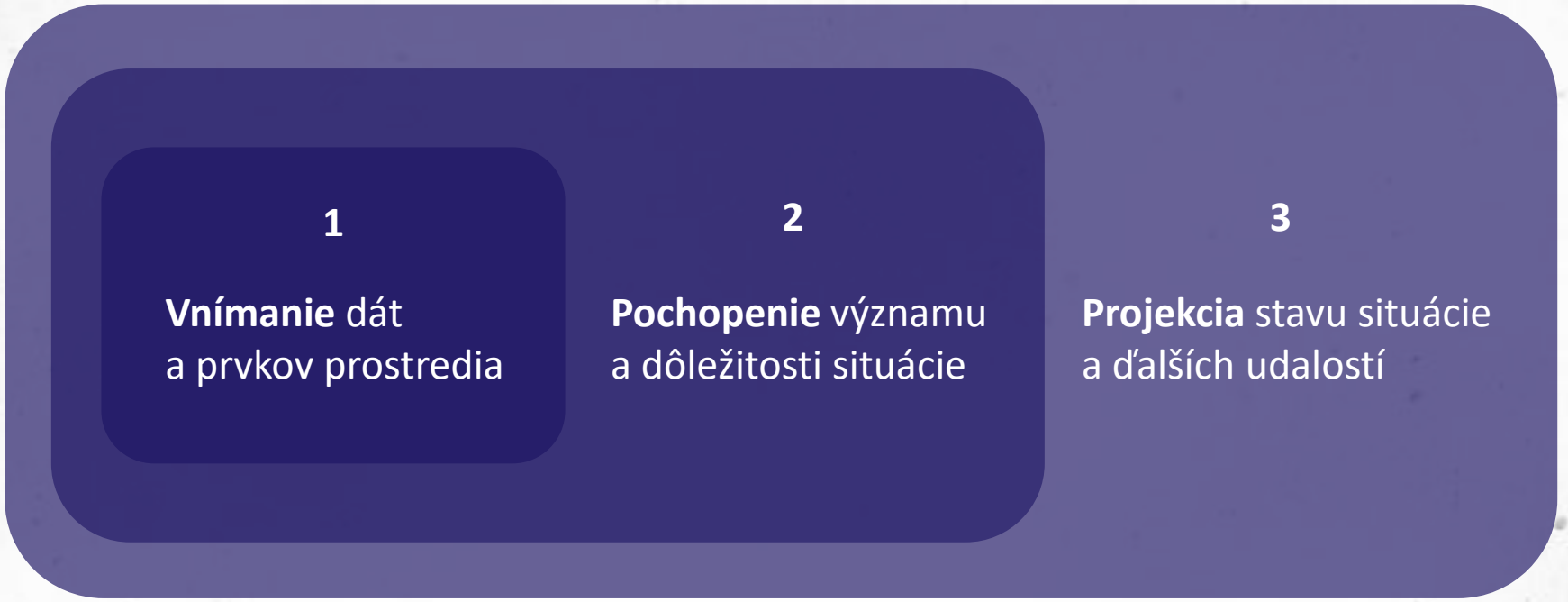
- Vnímanie prvkov v prostredí v danom časopriestore, pochopenie ich významu a projekcia ich blízkeho budúceho stavu
- Stav poznania

Situačné povedomie v kybernetickej bezpečnosti (Cyber Situational Awareness, **CSA**)

- Aplikácia situačného povedomia do kyberpriestoru

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

3 úrovne situačného povedomia



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

3 úrovne situačného povedomia

Úroveň 1 – Vnímanie

- Vnímanie prvkov, stavových atribútov a dynamiky relevantných atribútov v prostredí
- Správnosť vnímania zásadne ovplyvňuje celkový výsledok situačného povedomia (zaujatosť, nepresnosť vstupných dát vytvára o situácii mylný obraz)
- Bez interpretácie, len príjem informácií v „surovej“ forme
- Typický problém: „data overload“ – zahltenie objemom dát, prehliadnutie relevantných informácií

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

3 úrovne situačného povedomia

Úroveň 2 – Pochopenie

- Pochopenie vzniká syntézou jednotlivých prvkov zachytených na predošlej úrovni do koherentného, holistického obrazu prostredia
- Prvky sa kombinujú, interpretujú a priraďuje sa im význam vo vzťahu ku konkrétnym cieľom
- Dôležitá je znalosť/odbornosť operátora

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

3 úrovne situačného povedomia

Úroveň 3 – Projekcia

- Projekcia odhaduje budúci stav prvkov prostredia na základe aktuálnych udalostí a ich dynamiky
- Umožňuje robiť včasné rozhodnutia
- Ilustračný príklad: skúsený vodič predvída dopravnú situáciu a predchádza kolíziám (analógia k operátorovi, ktorý včas odhadne eskalujúci incident)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Špecifiká CSA

- **Kyberpriestor** nemá prirodzené hranice, jeho možnosti sú „neobmedzené“ (na rozdiel od fyzického sveta viazaného fyzikálnymi zákonmi) – v CSA sa preto zvyknú priestorové hranice vymedziť fyzickým umiestnením siete/systému
- Všetky informácie sú získané výhradne cez hardvérové senzory, nevieme ich overiť fyzickým/priamym pozorovaním
- Relatívne malé požiadavky na útok (možné aj na úrovni jednotlivca), rýchly sled udalostí počas útoku, spracovanie veľkého objemu informácií v CSA
- Výhody pre útočníka: anonymita, globálny dosah, sociálne inžinierstvo využívajúce ľudskú slabosť, ...

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Entity CSA

Tvoria kyberpriestor, navzájom interagujú a spolu ovplyvňujú tvorbu CSA

Fyzické entity

- Hardvérové a infraštruktúrne prvky – počítače a ich periférié, routre, switche, ...
- Nadobúdajú špecifické roly (napr. počítač ako pracovná stanica vs. server)

Nehmotné entity

- Softvérové a virtuálne prvky – programy, sieťové služby
- Slúžia na komunikáciu medzi človekom a počítačom, alebo počítačmi navzájom

Ľudské entity

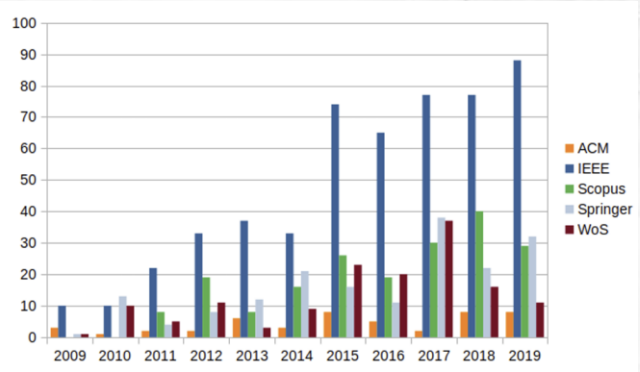
- Ľudia interagujúci s počítačmi
- 2 hlavné roly: útočník a obranca (bezpečnostný analytik/architekt/inžinier, ...)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSA výskum

- Rastúci počet publikácií na tému CSA
- Rastúci trend aplikovaného výskumu a experimentálneho vývoja (najznámejšie nástroje navrhla organizácia MITRE, napr. CyGraph)

Počet publikovaných príspevkov



Zdroj: M. Husák, T. Jirsík, and S. J. Yang, "SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security," in *Proc. 15th Int. Conf. Availability, Reliability and Security (ARES)*, Virtual Event, Ireland, Aug. 25–28, 2020, pp. 1–10, doi: 10.1145/3407023.3407062.

Kľúčové referenčné zdroje:

- *Cyber Situational Awareness: Issues and Research* (ed. Jajodia a kol., 2010)
- *Cyber Defense and Situational Awareness* (Kott a kol., 2014)

Prehľad pokrokov vo výskume:

- *Theory and Models for Cyber Situation Awareness* (Liu a kol., 2017)

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSA výskumné skupiny

- George Mason University (Jajodia)
- U.S. Army Research Laboratory (Kott)
- Rochester Institute of Technology (Yang)
- Swedish Defense Research Agency + RISE SICS (Brynielsson, Franke)
- AIT Austrian Institute of Technology (Skopik)
- CSIRT na Masarykovej univerzite

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Dáta na CSA výskum

Hlavný problém vo výskume: nedostatok datasetov s „ground truth“

Typy datasetov:

- **Umelé/syntetické datasety**
  + majú „ground truth“, dokumentáciu (topológia siete, zámery útočníkov, scenáre)
  - často chýba realistický „background traffic“, šum, anomálie, neznáme hrozby
- **Live datasety**
  + bližšie reálnym potrebám výskumníkov
  - chýba „ground truth“ (ťažké jednoznačne priradiť príčinu/úmysel), nutná anonymizácia

Oba typy datasetov rýchlo zastarávajú (nové techniky, nástroje, AI, ...)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Dáta na CSA výskum

Väčšina datasetov obsahuje stopy sieťovej prevádzky používané na detekciu prienikov (IDS), len niektoré obsahujú aj pravidlá na detekciu prienikov (IDS rules) a topológiu siete pre CSA výskum

- DARPA datasety – najznámejšie, v minulosti veľmi populárne, dnes považované za zastaralé
- CTU-13, UNB (University of New Brunswick) datasety – novšie, populárne
- SABU dataset (live) – vhodný na testovanie korelácie alertov medzi viacerými účastníkmi
- CAIDA (live) – dáta zo sieťového teleskopu a ďalších senzorov
- MM-TBM dataset (umelý) – obsahuje topológiu siete a šum

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Súčasné výzvy pre CSA

Dáta

- Obrovské množstvo dát, ktoré v surovej forme nedáva operátorovi význam („data overload – meaning underload“)
- Vysoká rýchlosť prichádzajúcich dát je kombinovaná s požiadavkou na analýzu v reálnom čase, nástroje na spracovanie a analýzu dát musia bežať veľmi rýchlo
- Dôraz na správne časové usporiadanie dát, keďže udalosti v kyberpriestore môžu nastať v milisekundových intervaloch (správne časové zoradenie udalostí je nevyhnutné pri analýzach, kde nás zaujíma kauzalita)
- Z veľkého množstva dát tvorí škodlivú aktivitu len malé množstvo alertov, čo vedie k extrémne vysokému pomeru šumu k signálu
- Rôznorodosť dát prináša výzvy pri zjednocovaní údajov z rôznych zdrojov a rôznych typov dát

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

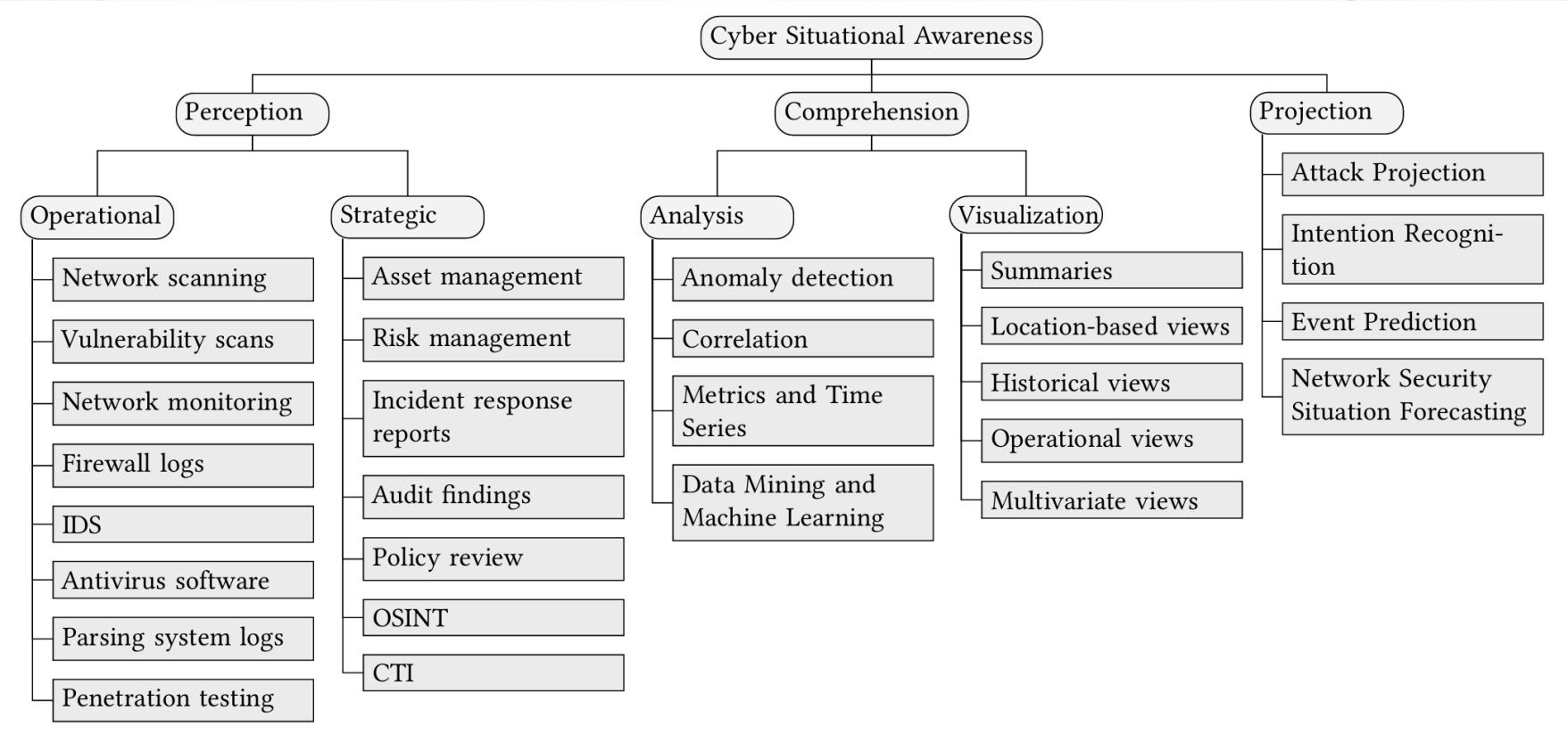
Súčasné výzvy pre CSA

Nástroje

- Na spracovanie dát z rôznych zdrojov sú potrebné rôzne nástroje (prepínanie medzi nástrojmi, manuálne náročné)
- Vizualizácia zohráva kľúčovú úlohu pri pochopení situácie
- Otvorený problém – vizualizácia rozsiahlych a dynamicky sa meniacich sietí
- Aktuálne výzvy – škálovateľnosť a priepustnosť nástrojov, skrátenie času analýzy a času odozvy (operátor potrebuje nové informácie čo najskôr, aby dokázal včas reagovať)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Taxonómia a komponenty CSA



Zdroj: M. Husák, T. Jirsík, and S. J. Yang, "SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security," in *Proc. 15th Int. Conf. Availability, Reliability and Security (ARES)*, Virtual Event, Ireland, Aug. 25–28, 2020, pp. 1–10, doi: 10.1145/3407023.3407062.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Taxonómia a komponenty CSA

Vnímanie

- Operačné – krátke časové horizonty pri každodennom riešení incidentov; zdroje ako sieťová prevádzka, výstupy z IDS, systémové logy, ...
- Strategické – dlhšie časové horizonty; zdroje ako správy z reakcií na incidenty, zistenia z auditov, OSINT, CTI, ...

Pochopenie

- Analýza – skúma a interpretuje zozbierané údaje; zahŕňa detekciu anomálií, koreláciu alertov/udalostí, metriky, časové rady, dolovanie dát, strojové učenie
- Vizualizácia – premieňa výsledky analýzy na situačné prehľady; zahŕňa súhrny a lokalizačné, historické, operačné, viacdimenzionálne prehľady

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Taxonómia a komponenty CSA

Projekcia

- Projekcia útoku a rozpoznávanie zámeru – cieľom je odhadnúť aký bude ďalší krok útočníka / ako sa útok bude pravdepodobne ďalej vyvíjať + aký cieľ útočník sleduje
- Predikcia prienikov – cieľom je odhadnúť budúce útoky alebo bezpečnostné incidenty aj bez toho, aby už bol rozpoznaný prebiehajúci viacstupňový útok
- Predpovedanie bezpečnostnej situácie v sieti – zameriava sa na budúci stav bezpečnostnej situácie siete alebo prostredia, môže ísť napr. o predikciu počtu incidentov, intenzity útokov, vývoja zraniteľností

V kybernetickej bezpečnosti nestačí útoky iba detegovať a reagovať na ne až po ich vzniku – kľúčová je schopnosť **predvídať** ďalší vývoj útoku, odhadnúť jeho cieľ alebo budúci stav bezpečnostnej situácie v sieti

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Projekcia

Metódy založené na diskrétnych modeloch

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Grafy útoku

- Graf útoku – grafické znázornenie scenára útoku
- Stali sa základom aj pre ďalšie prístupy založené na kontrole modelov – napr. pre metódy využívajúce Bayesovské siete, Markovove modely a metódy založené na teórii hier

Graf $G = (S, r, S_0, S_s)$, kde:

- S je množina stavov,
- $r \subseteq S \times S$ je prechodová relácia (možné akcie útočníka, zvyčajne ohodnotené, napr. pravdepodobnosťou že si útočník zvolí danú akciu)
- $S_0 \subseteq S$ je množina počiatočných stavov
- $S_s \subseteq S$ je množina úspešných stavov

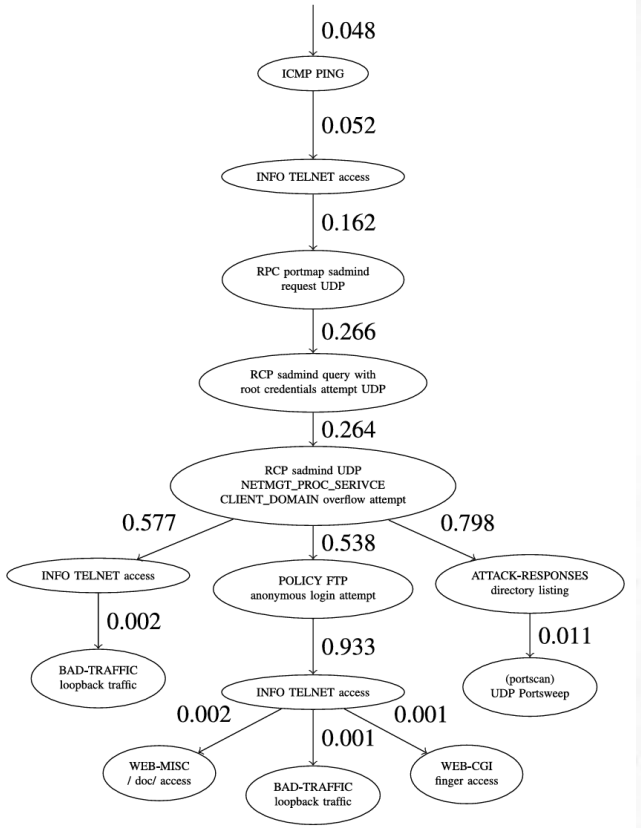
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Grafy útoku

Príklad grafu útoku

- Uzly – možné udalosti, ktoré tvoria útok
- Hodnoty na hranách – pravdepodobnosť, s akou nastane udalosť priradená ku koncovému uzlu

Predikcie pomocou grafov útoku sú založené na prechádzaní grafu a hľadaní úspešnej cesty útoku alebo na pravdepodobnostných hodnotách hrán



Zdroj: M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Grafy útoku – prehľad výskumu

T. Hughes and O. Sheyner, "**Attack scenario graphs for computer network threat analysis and prediction**," Complexity, vol. 9, no. 2, pp. 15–18, 2003.

C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "**NICE: Network intrusion detection and countermeasure selection in virtual network systems**," IEEE Trans. Depend. Secure Comput., vol. 10, no. 4, pp. 198–211, Jul./Aug. 2013.

I. Kotenko and A. Chechulin, "**A cyber attack modeling and impact assessment framework**," in Proc. 5th Int. Conf. Cyber Conflict (CYCON), Jun. 2013, pp. 1–24.

P. Cao, E. Badger, Z. Kalbarczyk, R. Iyer, and A. Slagell, "**Preemptive intrusion detection: Theoretical framework and real-world measure ments**," in Proc. Symp. Bootcamp Sci. Security, Urbana, IL, USA, 2015, pp. 1–5.

A. A. Ramaki, M. Amini, and R. E. Atani, "**RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection**," Comput. Security, vol. 49, pp. 206–219, Mar. 2015.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Grafy útoku – prehľad výskumu

M. GhasemiGol, A. Ghaemi-Bafghi, and H. Takabi, "**A comprehensive approach for network attack forecasting**," Comput. Security, vol. 58, pp. 83–105, May 2016.

M. GhasemiGol, H. Takabi, and A. Ghaemi-Bafghi, "**A foresight model for intrusion response management**," Comput. Security, vol. 62, pp. 73–94, Sep. 2016.

N. Polatidis, E. Pimenidis, M. Pavlidis, and H. Mouratidis, "**Recommender systems meeting security: From product recommenda tion to cyber-attack prediction**," in Engineering Applications of Neural Networks. Cham, Switzerland: Springer Int., 2017, pp. 508–519.

N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis, "**From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks**," in Evolving Systems. Heidelberg, Germany: Springer, May 2018.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

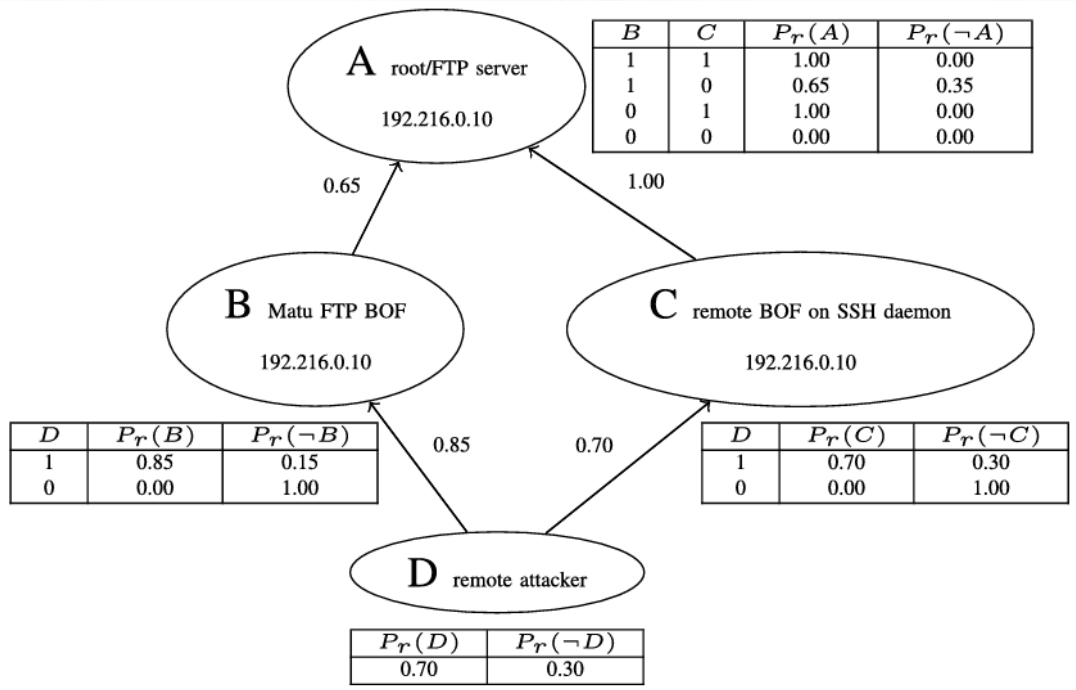
Bayesovské siete

- Pravdepodobnostný grafický model
- Sieť je orientovaný acyklický graf, kde uzly predstavujú diskrétne alebo spojité náhodné premenné a hrany vzťahy medzi nimi
- Uzly uchovávajú stavy náhodných premenných a podmienené pravdepodobnosti
- Na vytvorenie Bayesovskej siete / Bayesovského grafu útoku je potrebný zoznam udalostí, kauzálne závislosti medzi udalosťami a pravdepodobnosti prechodov medzi udalosťami
- Predikcia alertov využíva pravdepodobnosti zachytené v modeli

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bayesovské siete

Príklad Bayesovského grafu útoku



B	C	$Pr(A)$	$Pr(\neg A)$
1	1	1.00	0.00
1	0	0.65	0.35
0	1	1.00	0.00
0	0	0.00	0.00

D	$Pr(B)$	$Pr(\neg B)$
1	0.85	0.15
0	0.00	1.00

D	$Pr(C)$	$Pr(\neg C)$
1	0.70	0.30
0	0.00	1.00

$Pr(D)$	$Pr(\neg D)$
0.70	0.30

Zdroj: M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bayesovské siete – prehľad výskumu

X. Qin and W. Lee, “**Attack plan recognition and prediction using causal networks**,” in Proc. 20th Annu. Comput. Security Appl. Conf., Dec. 2004, pp. 370–379.

J. Wu, L. Yin, and Y. Guo, “**Cyber attacks prediction model based on Bayesian network**,” in Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst. (ICPADS), Dec. 2012, pp. 730–731.

A. A. Ramaki, M. Khosravi-Farmad, and A. G. Bafghi, “**Real time alert correlation and prediction using Bayesian networks**,” in Proc. IEEE 12th Int. Iran. Soc. Cryptol. Conf. Inf. Security Cryptol. (ISCISC), 2015, pp. 98–103.

A. Okutan, S. J. Yang, and K. McConky, “**Predicting cyber attacks with Bayesian networks using unconventional signals**,” in Proc. 12th Annu. Conf. Cyber Inf. Security Res., 2017, pp. 1–13.

K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, “**Assessing the physical impact of cyberattacks on industrial cyber-physical systems**,” IEEE Trans. Ind. Electron., vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

Financované Európskou úniou
NextGenerationEU

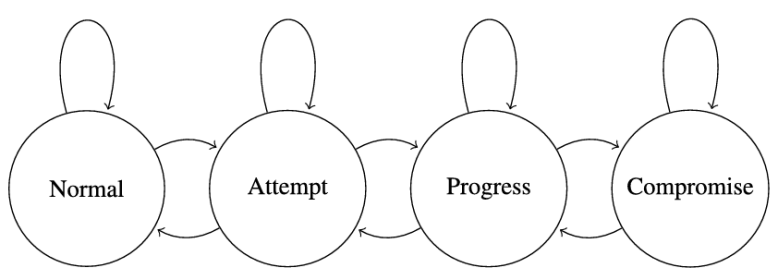
PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Markovove modely

- Reprezentované vo forme grafu
- Fungujú dobre aj v prítomnosti nepozorovateľných stavov a prechodov – umožňujú detekciu prienikov aj keď niektoré kroky útoku neboli zachytené
- Existuje viacero variantov Markovových modelov používaných na predikciu útokov, napr. skryté Markovove modely (HMM), Markovove modely s premenlivou dĺžkou (VLMM) a Markovove modely s premenlivým rádom (VOMM)
- V kyberbezpečnosti predstavujú uzly triedy útokov, hrany pozorovacie symboly a váhy hrán pravdepodobnosti

Príklad HMM na predikciu útokov



Zdroj: M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Markovove modely – prehľad výskumu

H. Farhadi, M. AmirHaeri, and M. Khansari, "**Alert correlation and prediction using data mining and HMM**," ISeCure, vol. 3, no. 2, pp. 77–101, 2011.

A. S. Sendi, M. Dagenais, M. Jabbarifar, and M. Couture, "**Real time intrusion prediction based on optimized alerts with hidden Markov model**," J. Netw., vol. 7, no. 2, pp. 311–321, 2012.

S. Shin, S. Lee, H. Kim, and S. Kim, "**Advanced probabilistic approach for network intrusion forecasting and detection**," Expert Syst. Appl., vol. 40, no. 1, pp. 315–322, 2013.

Y. Zhang, D. Zhao, and J. Liu, "**The application of Baum–Welch algorithm in multistep attack**," Sci. World J., vol. 2014, May 2014, Art. no. 374260.

H. A. Kholidy, A. Erradi, S. Abdelwahed, and A. Azab, "**A finite state hidden Markov model for predicting multistage attacks in cloud systems**," in Proc. IEEE 12th Int. Conf. Depend. Auton. Secure Comput. (DASC), Aug. 2014, pp. 14–19.

H. A. Kholidy, A. M. Yousof, A. Erradi, S. Abdelwahed, and H. A. Ali, "**A finite context intrusion prediction model for cloud systems with a probabilistic suffix tree**," in Proc. Eur. Model. Symp. (EMS), Oct. 2014, pp. 526–531.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Markovove modely – prehľad výskumu

S. Abraham and S. Nair, “**Exploitability analysis using predictive cybersecurity framework**,” in Proc. IEEE 2nd Int. Conf. Cybern. (CYBCONF), Jun. 2015, pp. 317–323.

A. Bar, B. Shapira, L. Rokach, and M. Unger, “**Identifying attack propagation patterns in honeypots using Markov chains modeling and complex networks analysis**,” in Proc. IEEE Int. Conf. Softw. Sci. Technol. Eng. (SWSTE), 2016, pp. 28–36.

A. Bar, B. Shapira, L. Rokach, and M. Unger, “**Scalable attack propagation model and algorithms for honeypot systems**,” in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2016, pp. 1130–1135.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Teória hier

- Hra ako model interakcie medzi útočníkom a obrancom
- Hľadanie najlepšej stratégie pre hráčov
- Základné predpoklady teórie hier: účastníci sú racionálni a uvažujú strategicky

Hra pozostáva z:

- konečnej množiny N hráčov (v kontexte sieťovej bezpečnosti zvyčajne útočník a obranca/správca)
- neprázdnej množiny akcií A_i pre každého hráča $i \in N$
- výplatnej funkcie u_i pre každého hráča $i \in N$, ktorá každému výsledku $a \in \times_{j \in N} A_j$ priraďuje úžitok hráča i

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Teória hier – prehľad výskumu

V. Lisý, R. Píbil, J. Stiborek, B. Bosanský, and M. Pechoucek, "**Game theoretic approach to adversarial plan recognition**," in Proc. ECAI, 2012, pp. 546–551.

R. Píbil, V. Lisý, C. Kiekintveld, B. Bošanský, and M. Pěchouček, "**Game theoretic model of strategic honeypot selection in computer networks**," in Decision and Game Theory for Security. Heidelberg, Germany: Springer, 2012, pp. 201–220.

M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, "**A system for intrusion prediction in cloud computing**," in Proc. Int. Conf. Internet Things Cloud Comput., Cambridge, U.K., 2016, pp. 1–35.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Projekcia

Metódy založené na spojitých modeloch

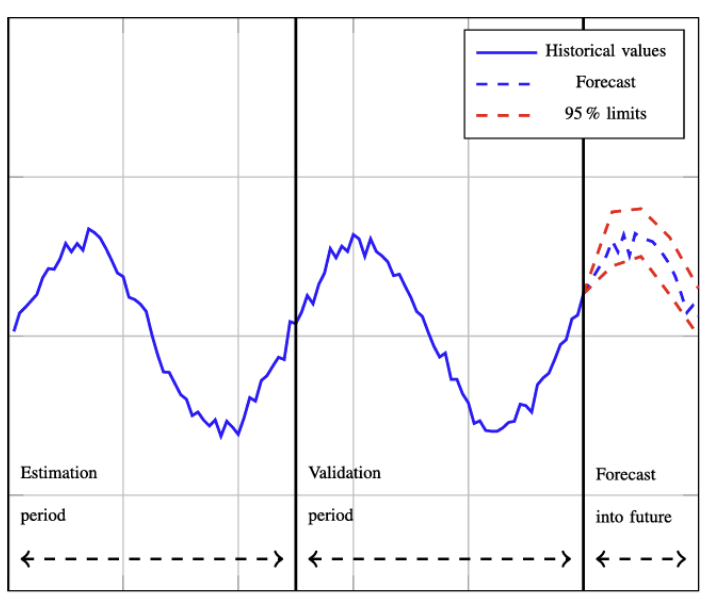
Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Časové rady

- Časový rad – množina po sebe nasledujúcich dátových bodov usporiadaných podľa času
- Často sú reprezentované vo forme čiarového grafu
- Zachytávajú vývoj v čase a umožňujú odhadovať budúce hodnoty na základe historických pozorovaní
- Predikujú skôr numerické charakteristiky bezpečnostnej situácie než konkrétne kroky útočníka
- Často sa používajú aj pri detekcii anomálií
- Na analýzu časových radov existujú rôzne metódy, napr. kĺzavý priemer, autoregresné modely s kĺzavým priemerom



Príklad časového radu

Zdroj: M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Časové rady – prehľad výskumu

H. Park, S.-O. D. Jung, H. Lee, and H. P. In, "**Cyber weather forecasting: Forecasting unknown Internet worms using randomness analysis**," in Information Security and Privacy Research. Heidelberg, Germany: Springer, 2012, pp. 376–387.

Z. Zhan, M. Xu, and S. Xu, "**Characterizing honeypot-captured cyber attacks: Statistical framework and case study**," IEEE Trans. Inf. Forensics Security, vol. 8, no. 11, pp. 1775–1789, Nov. 2013.

A. Silva, E. Pontes, F. Zhou, A. Guelf, and S. Kofuji, "**PRBS/EWMA based model for predicting burst attacks (Brute Froce, DoS) in computer networks**," in Proc. 9th Int. Conf. Digit. Inf. Manag. (ICDIM 2014), Sep./Oct. 2014, pp. 194–200.

A. B. Abdullah, T. R. Pillai, and L. Z. Cai, "**Intrusion detection forecasting using time series for improving cyber defence**," Int. J. Intell. Syst. Appl. Eng., vol. 3, no. 1, pp. 28–33, 2015.

T. R. Pillai, S. Palaniappan, A. Abdullah, and H. M. Imran, "**Predictive modeling for intrusions in communication systems using GARMA and ARMA models**," in Proc. 5th Nat. Symp. Inf. Technol. Towards New Smart World (NSITNSW), Feb. 2015, pp. 1–6.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Časové rady – prehľad výskumu

J. Freudiger, E. De Cristofaro, and A. E. Brito, "**Controlled Data Sharing for Collaborative Predictive Blacklisting**," in Detection of Intrusions and Malware, and Vulnerability Assessment, Cham, Switzerland: Springer International Publishing, 2015, pp. 327–349.

Y.-Z. Chen, Z.-G. Huang, S. Xu, and Y.-C. Lai, "**Spatiotemporal patterns and predictability of cyberattacks**," PLoS ONE, vol. 10, no. 6, Jun. 2015, Art. no. e0131501.

Z. Zhan, M. Xu, and S. Xu, "**Predicting cyber attack rates with extreme values**," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1666–1677, Aug. 2015.

P. Sokol and A. Gajdoš, "**Prediction of Attacks Against Honeynet Based on Time Series Modeling**," in Applied Computational Intelligence and Mathematical Methods, Cham, Switzerland: Springer International Publishing, 2018, pp. 360–371.

G. Werner, S. Yang, and K. McConky, "**Time series forecasting of cyber attack intensity**," in Proc. 12th Annu. Conf. Cyber Inf. Security Res., Oak Ridge, TN, USA, 2017, pp. 1–18.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Časové rady – prehľad výskumu

S. Dowling, M. Schukat, and H. Melvin, “**Using analysis of temporal variances within a honeypot dataset to better predict attack type probability**,” in Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST), Dec. 2017, pp. 349–354.

A. Okutan, G. Werner, K. McConky, and S. J. Yang, “**POSTER: Cyber attack prediction of threats from unconventional resources (CAPTURE)**,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security, Dallas, TX, USA, 2017, pp. 2563–2565.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sivé modely

- Používajú sa na predikciu kyberbezpečnostnej situácie
- V tejto teórii sa situácia bez informácií označuje ako čierna, situácia s úplnými informáciami ako biela, a keďže sa reálne problémy nachádzajú niekde medzi nimi, táto situácia sa označuje ako sivá – môžeme ju modelovať pomocou sivého modelu
- Najpoužívanejšie sivé modely: GM(1,1) a jeho modifikácia Grey-Verhulst model

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sivé modely – prehľad výskumu

Z. Lin, L. Xiujie, M. Jing, S. Wenchang, and W. Xiufang, "**The prediction algorithm of network security situation based on Grey correlation entropy Kalman filtering**," in Proc. IEEE 7th Joint Int. Inf. Technol. Artif. Intell. Conf. (ITAIC), Dec. 2014, pp. 321–324.

Y.-B. Leau and S. Manickam, "**A novel adaptive Grey Verhulst model for network security situation prediction**," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 90–95, 2016.

Y.-B. Leau and S. Manickam, "**An enhanced adaptive Grey Verhulst prediction model for network security situation**," Int. J. Comput. Sci. Netw. Security (IJCSNS), vol. 16, no. 5, pp. 13–20, 2016.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Projekcia

Metódy založené na strojovom učení a dolovaní dát

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metódy strojového učenia

- Na predikciu budúcich udalostí (napr. kybernetické útoky) je možné použiť rôzne metódy strojového učenia
- Najčastejšie používaná forma strojového učenia – neurónové siete

Proces aplikácie metód strojového učenia pozostáva z dvoch fáz:

- Trénovacia – model sa učí na príkladoch z trénovacieho datasetu
- Testovacia – model spracuje nové dáta a vráti pre ne výsledky

Typy učenia:

- Učenie bez učiteľa – model sa učí autonómne, bez označených vstupných dát
- Učenie s učiteľom – vstupné dáta sú označené ľudským expertom
- Poloriadené učenie (semi-supervised learning) – označená je iba časť vstupných dát

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Neurónové siete – prehľad výskumu

R. Zheng, D. Zhang, Q. Wu, M. Zhang, and C. Yang, "**A strategy of network security situation autonomic awareness**," in Network Computing and Information Security. Heidelberg, Germany: Springer, 2012, pp. 632–639.

F. Chen, Y. Shen, G. Zhang, and X. Liu, "**The network security situation predicting technology based on the small-world echo state network**," in Proc. 4th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS), 2013, pp. 377–380.

Y. Zhang, S. Jin, X. Cui, X. Yin, and Y. Pang, "**Network security situation prediction based on BP and RBF neural network**," in Trustworthy Computing and Services. Berlin, Heidelberg: Springer, 2013, pp. 659–665.

W. Xing-Zhu, "**Network intrusion prediction model based on RBF features classification**," Int. J. Security Appl., vol. 10, no. 4, pp. 241–248, 2016.

H. Zhang, Q. Huang, F. Li, and J. Zhu, "**A network security situation prediction model based on wavelet neural network with optimized parameters**," Digit. Commun. Netw., vol. 2, no. 3, pp. 139–144, 2016.

F. He et al., "**Mixed wavelet-based neural network model for cyber security situation prediction using MODWT and Hurst exponent analysis**," in Network and System Security. Cham, Switzerland: Springer Int., 2017, pp. 99–111.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metóda podporných vektorov – prehľad výskumu

X. Cheng and S. Lang, "**Research on network security situation assessment and prediction**," in Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCIS), 2012, pp. 864–867.

G. K. Jayasinghe, J. S. Culpepper, and P. Bertok, "**Efficient and effective realtime prediction of drive-by download attacks**," J. Netw. Comput. Appl., vol. 38, pp. 135–149, Feb. 2014.

S. O. Uwagbole, W. J. Buchanan, and L. Fan, "**Applied machine learning predictive analytics to SQL injection attack detection and prevention**," in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM), May 2017, pp. 1087–1090.

S. O. Uwagbole, W. J. Buchanan, and L. Fan, "**An applied pattern driven corpus to predictive analytics in mitigating SQL injection attack**," in Proc. 7th Int. Conf. Emerg. Security Technol. (EST), Sep. 2017, pp. 12–17.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Dolovanie dát – prehľad výskumu

C. Fachkha et al., “**Investigating the dark cyberspace: Profiling, threat based analysis and correlation**,” in Proc. 7th Int. Conf. Risks Security Internet Syst. (CRiSIS), Oct. 2012, pp. 1–8.

Y.-H. Kim and W. H. Park, “**A study on cyber threat prediction based on intrusion detection event for APT attack detection**,” Multimedia Tools Appl., vol. 71, no. 2, pp. 685–698, Jul. 2014.

M. Husák and J. Kašpar, “**Towards predicting cyber attacks using information exchange and data mining**,” in Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2018, pp. 536–541.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Iné metódy strojového učenia – prehľad výskumu

Rozhodovací strom

K. Soska and N. Christin, "**Automatically detecting vulnerable websites before they turn malicious**," in Proc. USENIX Security Symp., 2014, pp. 625–640.

Náhodný les

Y. Liu et al., "**Cloudy with a chance of breach: Forecasting cyber security incidents**," in Proc. USENIX Security Symp., Washington, DC, USA, 2015, pp. 1009–1024.

Dolovanie pravidiel, zhlukovanie

P. Shao, J. Lu, R. K. Wong, and W. Yang, "**A transparent learning approach for attack prediction based on user behavior analysis**," in Information and Communications Security. Cham, Switzerland: Springer Int., 2016, pp. 159–172.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Iné metódy strojového učenia – prehľad výskumu

Kombinácia metód učenia s učiteľom a bez učiteľa

K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, "**AI2: Training a big data machine to defend**," in Proc. IEEE 2nd Int. Conf. Big Data Security Cloud (BigDataSecurity) IEEE Int. Conf. High Perform. Smart Comput. (HPSC) IEEE Int. Conf. Intell. Data Security (IDS), New York, NY, USA, Apr. 2016, pp. 49–54.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Projekcia

Iné prístupy

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prístupy založené na podobnosti – prehľad výskumu

A. Jantan, M. Rasmi, M. I. Ibrahim, and A. H. A. Rahman, "**A similarity model to estimate attack strategy based on intentions analysis for network forensics**," in Recent Trends in Computer Networks and Distributed Systems Security. Berlin, Heidelberg: Springer, 2012, pp. 336–346.

M. Rasmi and A. Jantan, "**A new algorithm to estimate the similarity between the intentions of the cyber crimes for network forensics**," Procedia Technol., vol. 11, pp. 540–547, 2013.

A. AlEroud and G. Karabatis, "**Context infusion in semantic link networks to detect cyber-attacks: A flow-based detection approach**," in Proc. IEEE Int. Conf. Semantic Comput., Jun. 2014, pp. 175–182.

A. AlEroud and G. Karabatis, "**Methods and techniques to identify security incidents using domain knowledge and contextual information**," in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM), May 2017, pp. 1040–1045.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prístupy založené na podobnosti – prehľad výskumu

C.-B. Jiang, I.-H. Liu, Y.-N. Chung, and J.-S. Li, "**Novel intrusion prediction mechanism based on honeypot log similarity**," Int. J. Netw. Manag., vol. 26, on. 3, pp. 156–175, 2016.

A. AlEroud and I. Alsmadi, "**Identifying cyber-attacks on software defined networks: An inference-based intrusion detection approach**," J. Netw. Comput. Appl., vol. 80, pp. 152–164, Feb. 2017.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Predikcia objemu DDoS útokov – prehľad výskumu

D. Kwon, J. W.-K. Hong, and H. Ju, "**DDoS attack forecasting system architecture using Honeynet**," in Proc. 14th Asia–Pac. Netw. Oper. Manag. Symp. (APNOMS), Sep. 2012, pp. 1–4.

D. Kwon, H. Kim, D. An, and H. Ju, "**DDoS attack volume forecasting using a statistical approach**," in Proc. TODO, 2017, pp. 1083–1086.

C. Fachkha, E. Bou-Harb, and M. Debbabi, "**Towards a forecasting model for distributed denial of service activities**," in Proc. 12th IEEE Int. Symp. Netw. Comput. Appl. (NCA), Cambridge, MA, USA, Aug. 2013, pp. 110–117.

A. Olabelurin, S. Veluru, A. Healing, and M. Rajarajan, "**Entropy clustering approach for improving forecasting in DDoS attacks**," in Proc. IEEE 12th Int. Conf. Netw. Sens. Control (ICNSC), Apr. 2015, pp. 315–320.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Evolučné výpočty – prehľad výskumu

G.-Y. Hu et al., “**A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm**,” Appl. Soft Comput., vol. 48, pp. 404–418, Nov. 2016.

G.-Y. Hu and P.-L. Qiao, “**Cloud belief rule base model for network security situation prediction**,” IEEE Commun. Lett., vol. 20, no. 5, pp. 914–917, May 2016.

H. Wei et al., “**A new BRB model for cloud security-state prediction based on the large-scale monitoring data**,” IEEE Access, vol. 6, pp. 11907–11920, 2017.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Nekonvenčné zdroje dát – prehľad výskumu

A. Hernández et al., “**Security attack prediction based on user sentiment analysis of Twitter data**,” in Proc. IEEE Int. Conf. Ind. Technol. (ICIT), Mar. 2016, pp. 610–617.

A. Dalton, B. Dorr, L. Liang, and K. Hollingshead, “**Improving cyber-attack predictions through information foraging**,” in Proc. IEEE Int. Conf. Big Data (Big Data), Boston, MA, USA, Dec. 2017, pp. 4642–4647.

K. Shu, A. Sliva, J. Sampson, and H. Liu, “**Understanding cyber attack behaviors with sentiment information on social media**,” in Social, Cultural, and Behavioral Modeling. Cham, Switzerland: Springer Int., 2018, pp. 377–388.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Situačné povedomie v kybernetickej bezpečnosti

Zdroje:

- M. Husák, T. Jirsík, and S. J. Yang, “SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security,” in *Proc. 15th Int. Conf. Availability, Reliability and Security (ARES)*, Virtual Event, Ireland, Aug. 25–28, 2020, pp. 1–10, doi: 10.1145/3407023.3407062.
- M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, “Survey of Attack Projection, Prediction, and Forecasting in Cyber Security,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019, doi: 10.1109/COMST.2018.2871866.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY