

Vývoj kybernetickej bezpečnosti na Slovensku ako reakcia na vnútorné a vonkajšie ohrozenia.

Daniel Mihályi

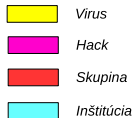
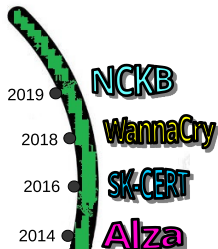
Ústav celoživotného vzdelávania a zahraničných štúdií
Vysoká škola bezpečnostného manažérstva v Košiciach



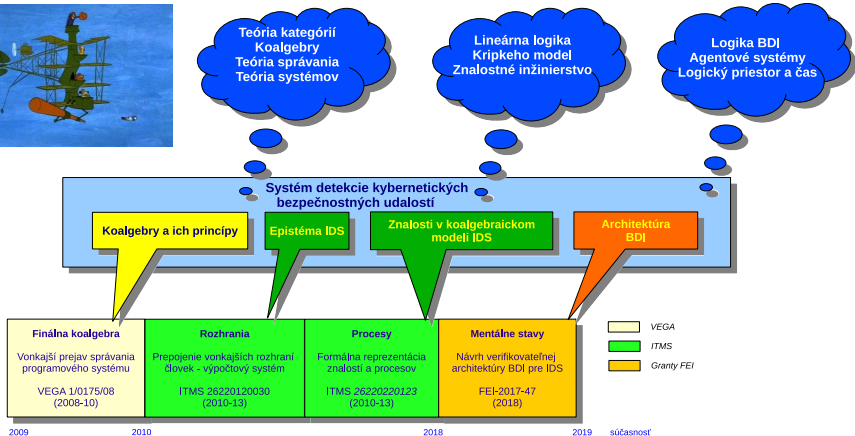
Podiplomová práca

18. júna 2021

Historické mílniky



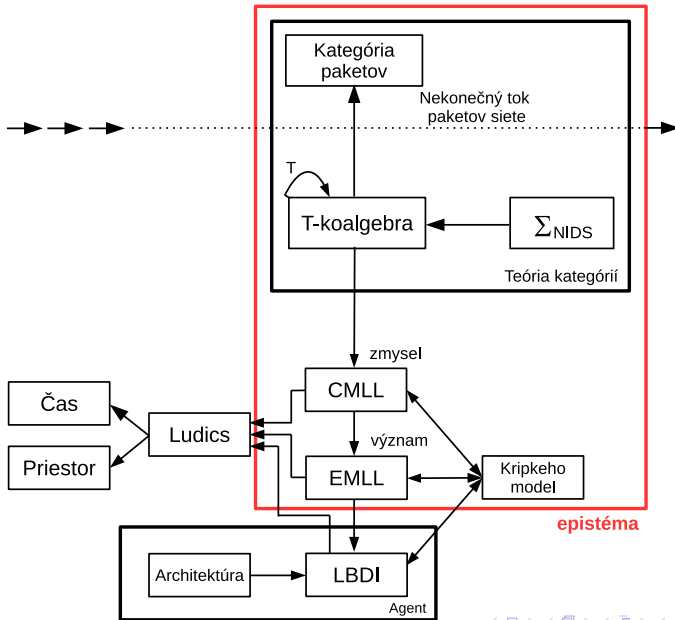
Chronológia výskumu



Výskum

- vnútorná štruktúra tvorenia konečných údajových štruktúr (štruktúra paketu),
- vonkajší prejav dynamického správania sa nekonečných údajových štruktúr (streamu paketov), zachytávaných koalgebrou potenčného endofunktora,
- zdrojovo orientovaný popis stavovo orientovanej dynamiky koalgebraická modálna lineárna logika,
- reprezentáciu znalostí na základe objektívneho poznania a racionálneho presvedčenia (logika nadobúdania znalostí agenta),
- logiku mentálnych stavov racionálneho agenta (jeho presvedčenia, prania a zámary),
- logický priestor a čas priebehu kybernetického incidentu (dizajn incidentu),

Výskum



Epistéma

BEGIN Signature

Σ_{nmap}

Begin types

$\mathcal{T} = \{action, flow, ipaddr, nat, natip, protocol, tcp_flags\}$

end

Begin opns

$\mathcal{F} = \{alert \rightarrow action$
 $tcp \rightarrow protocol$
 $exter_net \rightarrow natip, natip, natip, natip \rightarrow ipaddr$
 $home_net \rightarrow nat$
 $stateless \rightarrow flow$
 $attempted_recon \rightarrow class_type$
 $rev \rightarrow nat$
 $sid \rightarrow nat$

end

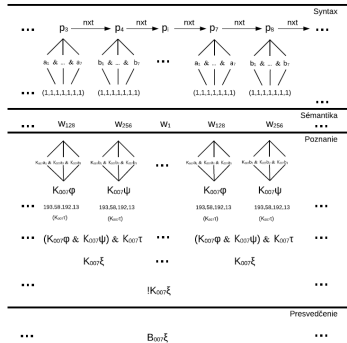
END

protocol	=	tcp
exter_net	=	any
home_net	=	161
flow	=	stateless
class_type	=	attempted - recon
rev	=	11
sid	=	1418

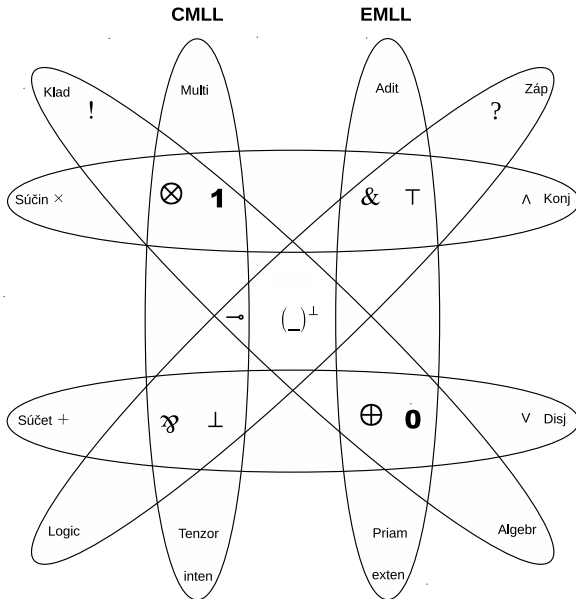
protocol	=	tcp
exter_net	=	any
home_net	=	705
flow	=	stateless
class_type	=	attempted - recon
rev	=	11
sid	=	1412

$(\rho_p, \langle hd, tl, intrusion_type \rangle)$

$\langle hd, tl, intrusion_type \rangle : \rho_p \rightarrow p \times \rho_p \times p^{actions^I}$



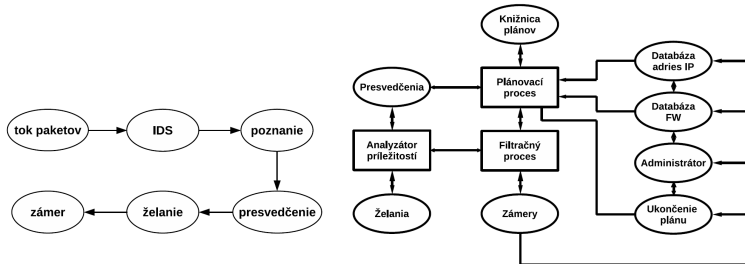
Lineárna logika



◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

$$\begin{array}{c}
\frac{}{\vdash N, \Gamma_1} \text{ (id)} \quad \frac{}{\vdash S_1, U_M, \Gamma_2} \text{ (id)} \\
\frac{}{\vdash N \otimes S_1^\perp, U_M, \Gamma_3} \text{ (}\otimes\text{r)} \quad \frac{}{\vdash N \otimes S_1^\perp, U_M, \Gamma_3} \text{ (}\otimes\text{r)} \\
\frac{}{\vdash (N \otimes S_1^\perp), U_M, \Gamma_3} \text{ (brac-r)} \\
\frac{}{(N \otimes S_1^\perp)^\perp \vdash U_M, \Gamma_3} \text{ (}\odot\text{)}^\perp \\
\frac{}{(N \otimes S_1^\perp)^\perp \vdash (U_M), \Gamma_3} \text{ (brac-r)} \\
\frac{}{(N \otimes S_1^\perp)^\perp \vdash \odot(U_M), \Gamma_3} \text{ (}\odot\text{r)} \\
\frac{}{(N \otimes S_1^\perp)^\perp \vdash \odot(U_M)^\perp \vdash \Gamma_3} \text{ (}\odot\text{)}^\perp \\
\frac{}{(N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp \vdash \Gamma_3} \text{ (}\otimes\text{)} \\
\frac{}{((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash \Gamma_3} \text{ (brac-l)} \\
\frac{}{((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash ((((((H_1^\perp \otimes H_2^\perp) \otimes H_3^\perp) \otimes H_4^\perp) \otimes H_5^\perp) \otimes S_2)^\perp \vdash \Gamma_5} \text{ (brac-l)} \\
\frac{}{(((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash ((((((H_1^\perp \otimes H_2^\perp) \otimes H_3^\perp) \otimes H_4^\perp) \otimes H_5^\perp) \otimes S_2)^\perp) \vdash \Gamma_5} \text{ (}\odot\text{)}^\perp \\
\frac{}{\vdash (((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash ((((((H_1^\perp \otimes H_2^\perp) \otimes H_3^\perp) \otimes H_4^\perp) \otimes H_5^\perp) \otimes S_2)^\perp)^\perp \vdash \Gamma_5} \text{ (}\odot\text{)}^\perp \\
\frac{}{\vdash (((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash ((((((H_1^\perp \otimes H_2^\perp) \otimes H_3^\perp) \otimes H_4^\perp) \otimes H_5^\perp) \otimes S_2)^\perp)^\perp \odot \odot(U_N)^\perp, \Gamma} \text{ (brac-r)} \\
\frac{}{\vdash (((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash ((((((H_1^\perp \otimes H_2^\perp) \otimes H_3^\perp) \otimes H_4^\perp) \otimes H_5^\perp) \otimes S_2)^\perp)^\perp \odot \odot(U_N)^\perp), \Gamma} \text{ (}\odot\text{)}^\perp \\
\frac{}{\vdash (((N \otimes S_1^\perp)^\perp \odot \odot(U_M)^\perp) \vdash ((((((H_1^\perp \otimes H_2^\perp) \otimes H_3^\perp) \otimes H_4^\perp) \otimes H_5^\perp) \otimes S_2)^\perp)^\perp \odot \odot(U_N)^\perp)^\perp \vdash \Gamma} \text{ (}\odot\text{)}^\perp
\end{array}$$

$$(((BEL_i(\varphi)) \otimes (DES_i(\psi) \otimes DES_i(\gamma) \otimes DES_i(\delta) \otimes DES_i(\omega) \otimes DES_i(\theta))) \multimap (INT_i(\psi) \otimes INT_i(\gamma) \otimes INT_i(\delta) \otimes INT_i(\omega) \otimes INT_i(\theta))) \multimap ((\psi) \otimes \gamma \otimes \delta \otimes \omega \otimes \theta)$$



ψ je plán porovnania cudzej adresy IP s položkami databázy blokových adries.

γ je plán pridania adresy IP útočníka do zoznamu blokových adries.

δ je plán pre zablokovanie prebiehajúcej komunikácie.

ω je plán kontaktovania správcu siete o vzniknutej udalosti.

θ je plán ukončenia činnosti agenta.

Prínosy/výsledky

AAB 1 Monografia, Equilibria Košice.

ADD 1 Karent, CAI, Bratislava.

ADE 3 Časopisy, Kluž, CEJCS.

ADF 1 Časopis AEI, FEI Tuke.

AED 4 Zborníky FEI/KPI Tuke.

AFD 2 Konferencie, Poprad,
Rožňava.

ADM 3 Indexované časopisy, Berlín,
Czestochowa, Budapešť.

DAI 2 Dizertačná práca Tuke.

4 Bakalárske záv. práce Tuke.

9 Inžinierske záv. práce Tuke.





Ďakujem za vzájomnú pozornosť :-)