Koalgebraické modelovanie správania sa IDS na zdrojovo orientovanom základe

Autor: Ján Perháč Vedúci diplomovej práce: Daniel Mihályi

Katedra počítačov a informatiky, Fakulta elektrotechniky a informatiky, Technická univerzita v Košiciach

Súčasné trendy

- Systém detekcie prienikov ako koalgebra polynomiálneho endofunktora.
- Použitie neklasického zdrojovo orientovaného systému na popis správania sa tohto programového systému v prípade výskytu sieťového narušenia resp. útoku.

Použité prostriedky, metódy, formalizmy

- Teória kategórií.
- Koalgebry.
- Neklasické logické systémy:
  - Koalgebraická logika.
  - Lineárna logika.
  - Modálna logika.
- Open source Intrusion Detection System (IDS) - *Snort*.
- Konfigurácia firewallu prostredníctvom linuxového systémového nástroja *iptables*.
- Sieťové nástroje pod OS Linux: *route, nmap, arpspoof, sslstrip*.

Koalgebraická modálna lineárna logika pre IDS (CMLL)

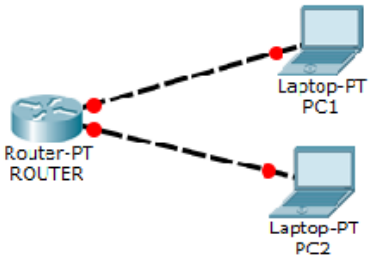
- Syntax, definovaná produkčným pravidlom v Backus-Naurovej forme:

$$\varphi ::= a_n \mid \mathbf{1} \mid \bot \mid \varphi \otimes \psi \mid \varphi \parr \psi \mid \varphi \multimap \psi \mid \varphi^{\bot} \mid \Box\varphi \mid \Diamond\varphi$$

- Sémantika, vyjadrená pomocou sémantiky možných svetov Kripkeho modelom.
- Dôkazový systém definovaný prostredníctvom dedukčných pravidiel Gentzenovho sekventového kalkulu.

Laboratórne prostredie

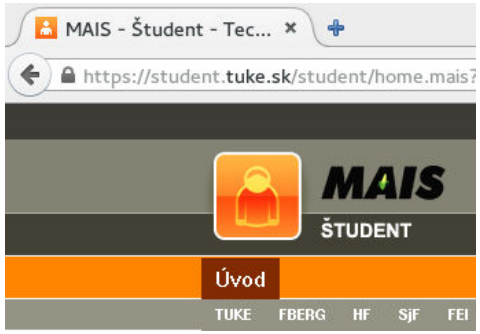
- Sieťová topológia laboratórneho prostredia:



- Simulácia narušení na dvoch hosťovských počítačoch (útočník, obeť) v rámci segmentu lokálnej počítačovej siete typu C.
- Realizácia kombinovaného skenu portov (narušenie siete) a sieťových útokov *ARP Spoofing* a *SSLStrip*.

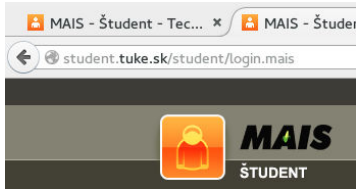
Rozhranie „Študent“ univerzitného portálu MAIS

- Univerzitný informačný systém.
- Komunikácia prostredníctvom HTTPS.
- Realizácia sieťového útoku na zabezpečenie *(šifrovanie)* komunikácie medzi používateľom a univerzitným portálom MAIS.



Informačný systém MAIS po realizácii reálneho sieťového útoku

- Odstránenie komunikácie prostredníctvom bezpečného protokolu HTTPS a jeho nahradenie za nešifrovaný protokol HTTP.



Formula CMLL útoku SSLStrip

- Priebeh útoku je vyjadrený formulou novo zavedeného logického systému:

$$(((P \otimes Ia_1) \multimap \Diamond At) \otimes ((A_1 \otimes A_2) \otimes Ia_2)) \multimap \Box At$$

- Formulu je možné prečítať ako: "kombinované skenovanie portov (P) spolu s akciou IDS vytvorenia logu (Ia_1) zapríčiní možný útok $(\Diamond At)$ a zároveň obojsmerné presmerovanie komunikácie cez klienta PC2 (útočníka) $(A_1 \otimes A_2)$ a akcia IDS vytvorením logu (Ia_2) zapríčiní reakciu, že útok nutne nastal $(\Box At)$"

Dôkaz behaviorálnej formuly CMLL v obojstrannom Gentzenovom sekventovom kalkule

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P, Ia_1, At \vdash P, Ia_1, At}\,(\mathrm{id})}{P, Ia_1, P^{\bot}, Ia_1^{\bot} \vdash At, At^{-}}\,((\cdot)^{\bot})}{P, Ia_1, P^{\bot}, Ia_1^{\bot} \vdash At, \Box(At^{-})}\,(\Box_r)}{P, Ia_1, P^{\bot}, Ia_1^{\bot} \vdash \Diamond At, \Box(At^{-})}\,(\Diamond_r)}{P \otimes Ia_1, P^{\bot}, Ia_1^{\bot} \vdash \Diamond At, \Box(At^{-})}\,(\otimes_l)}{\vdash (P \otimes Ia_1) \multimap \Diamond At, \Delta}\,(\multimap_r) \qquad \dfrac{\dfrac{\dfrac{}{A_1 \vdash A_1}\,(\mathrm{id})}{\vdash A_1, A_1^{-}}\,((\cdot)_r^{-1}) \qquad \dfrac{\dfrac{}{A_2 \vdash A_2}\,(\mathrm{id})}{\vdash A_2, A_2^{\bot}}\,((\cdot)_r^{\bot})}{\vdash A_1 \otimes A_2, A_1^{\bot}, A_2^{\bot}}\,(\otimes_r) \qquad \dfrac{\dfrac{}{Ia_2 \vdash Ia_2}\,(\mathrm{id})}{\vdash Ia_2, Ia_2^{\bot}}\,((\cdot)_r^{\bot})}{\vdash (A_1 \otimes A_2) \otimes Ia_2, \Psi}\,(\otimes_r)$$

$$\dfrac{\vdash ((P \otimes Ia_1) \multimap \Diamond At) \otimes ((A_1 \otimes A_2) \otimes Ia_2), \Sigma}{((P \otimes Ia_1) \multimap \Diamond At) \otimes ((A_1 \otimes A_2) \otimes Ia_2) \multimap \Box At \vdash \Gamma} \qquad \dfrac{\dfrac{\dfrac{}{At \vdash At}\,(\mathrm{id})}{\Box At \vdash At}\,(\Box_l)}{\Box At, At^{\bot} \vdash}\,((\cdot)^{\bot})}{\Box At, \Diamond(At^{\bot}) \vdash}\,(\Diamond_l)$$

Dosiahnuté výsledky

- Vyjadrenie mnohotypovej signatúry infikovaného paketu počítačovej siete obsahujúcej jeho štruktúru a charakteristickými znakmi jeho narušeného správania sa.
- Znázornenie nekonečného toku paketov v kategórii.
- Konštruovanie polynomiálneho endofunktora nad takouto kategóriou - abstraktný stavovo orientovaný popis správania sa IDS ako koalgebry polynomiálneho endofunktora.
- Zavedenie syntaxe, sémantiky a dôkazového kalkulu CMLL.
- Znázornenie behaviorálnej zdrojovo orientovanej formuly priebehu tohto útoku a realizácia jej dôkazu v dôkazovom kalkule Gentzenovského štýlu.
- Na základe skúmania symptómov útoku SSLStrip.
- Odhalenie bezpečnostnej chyby v informačnom systéme školy.
- Publikovanie výsledkov práce vo vedeckom časopise Acta Electrotechnica et Informatica (odoslané) a na medzinárodnej vedeckej konferencii Informatics 2015 (odoslané).