Rozšírené zadanie diplomovej práce

Názov: Časové osi pri forenznej analýze operačného systému Windows

Autor: Bc. Kristína Kováčová

Vedúci práce: RNDr. JUDr. Pavol Sokol, PhD.

Konzultant: Ing. Miroslav Sidor, CSIRT.SK

Pavol Sokol
Digitálne podpísal Pavol Sokol
Dátum: 2021.01.01 19:34:06 +01'00'

Ciele práce:

(1) Aktuálne prístupy k spracúvaniu časových osí forenzných artefaktov operačného systému Windows.
(2) Analýza spôsobov korelácie atribútov forenzných artefaktov a vytvárania vzťahov medzi nimi.
(3) Návrh, implementácia a vyhodnotenie nástroja pre vytvorenie a vizualizáciu časovej osi forenzných artefaktov operačného systému Windows.

Oblasť štúdia digitálnej forenznej analýzy sa za posledné roky stáva stále vyhľadávanejšou z dôvodu prudkého nárastu počítačových používateľov, elektronických zariadení, inovácií v technológiách a mnohých ďalších faktorov. Jej cieľom je nájsť a interpretovať pôvod nájdenej udalosti alebo artefaktu.

Pri digitálnej forenznej analýze je dôležité vedieť zostaviť časovú os aktivít v počítačovom systéme. Zo všeobecného hľadiska spočíva zostavenie časovej osi v zachytení systémových a sieťových udalostí a ich usporiadaní. Udalosťou rozumieme akúkoľvek aktivitu, od vytvorenia, modifikácie, až po odstránenie súboru, históriu webového prehliadača, prenos súborov, prihlásenie sa do emailových účtov a mnoho ďalších.

Prístupov a nástrojov k vytváraniu a spracúvaniu časových osí forenzných artefaktov operačného systému Windows existuje niekoľko. V našej práci sa budeme venovať ich porovnaniu a analýze v prvom z troch hlavných cieľov. Pri každom z jednotlivých nástrojov budeme porovnávať napríklad metódy spracovania udalostí, rýchlosť vytvorenia časovej osi, náročnosť použitia a taktiež ich výstup. Ich stručný prehľad nám poskytuje [2], v ktorom sú

taktiež priblížené problémy, ktoré je nutné riešiť pri analýze časových osí a taktiež popísaný nástroj Timeline2GUI.

Zhromažďovanie všetkých potrebných artefaktov a ich následné spracovanie predstavuje veľmi náročný proces z pohľadu objemu dát a ich heterogenity, a taktiež vybraného spôsobu ich spracovania. Na elimináciu nezaujímavých súborov sa používajú techniky zoskupovania údajov, ktoré urýchľujú proces vyšetrovania rýchlejším určením relevantných informácií. Z tohto dôvodu je primárnou úlohou zanalyzovať spôsob možnej korelácie atribútov vybraných artefaktov a určiť vzťahy medzi nimi. Práca na tomto cieli bude zahŕňať porovnanie existujúcich prístupov k tomuto problému, zostavenie vlastného riešenia a taktiež scenárov k určitým typom incidentov, na základe ktorých bude korelácia odskúšaná. Táto časť bude v našej práci mimoriadne dôležitá, pretože bude tvoriť základný pilier pre cieľ tretí.

Tretím cieľom je návrh a implementácia nástroja na vytváranie a vizualizáciu časovej osi forenzných artefaktov operačného systému Windows. V tomto cieli bude aj následne tento nástroj vyhodnotený. Požiadavky na výsledný produkt sú:

1. Dynamická vizualizácia,
2. Paralelné spracovanie udalostí,
3. Kolaboračný a zdieľaný prístup.

Literatúra:

(1) Carvey H.: Investigating Windows Systems, Academic Press, 1st edition, 2018.

(2) Debinski M., Breitinger F., Mohan P.: Timeline2GUI: A Log2Timeline CSV parser and training scenarios, Digital Investigation, Volume 28, Pages 34-43. 2019.

(3) Anson S.: Applied Incident Response, Wiley, 1st Edition, 2020.

(4) Osborne G., Thinyane H., Slay J.: Visualizing Information in Digital Forensics. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics VIII. DigitalForensics 2012. IFIP Advances in Information and Communication Technology, vol 383. Springer, Berlin, Heidelberg. 2012.