Dizajn sustava za bilježenje sistemskih i operativnih zapisa

Stjepan Groš, FER

Cyber Security Conference 2019

Osijek, 17. listopad 2019.

v2019101603

Pregled

Kontekst

Referentna arhitektura i njeno proširenje sigurnosnim elementima

Arhitektua Log sustava

Sigurnost sistemskih i operativnih zapisi

Savjeti za bolju suradnju istraživačkih institucija i tvrtki

Zaključak

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Kontekst

Materijal iznesen u ovoj prezentaciji rezultat je rada na IRI projektu čiji koordinator/prijavitelj je tvrtka SedamIT, a partner je FER

Projekt je započeo 15. 1. 2018. godine i traje do 15. 1. 2020.

Tim na FER-u ima dvije zadaće (dva podtima)

- Rad na snimanju mrežnog prometa pri brzinama 100Gbps
- Sigurnost arhitekture i komponenata arhitekture

U ovoj prezentaciji prikazani su neki rezultati rada na sigurnosti arhitekture i komponenata

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Postizanje povjerenja dionika u sigurnost sustava

Za ovako osjetljive sustave vrlo je bitno postići povjerenje dionika u njegovu sigurnost (engl. information assurance)

Postavljen kao jedan od vrlo bitnih ciljeva ovog sustava

Kako bi se to postiglo djeluje se u svim fazama životnog ciklusa sustava

Dizajn, implementacija, upogonjavanje (engl. deployment), održavanje, uklanjanje

Načini djelovanja su

Odgovarajuća dokumentacija, poslovni procesi, poseban naglasak na nadogradnje (updates)

Certifikacija ovakvih proizvoda za sada ne postoji (odnosno, nije nam poznato da postoji).

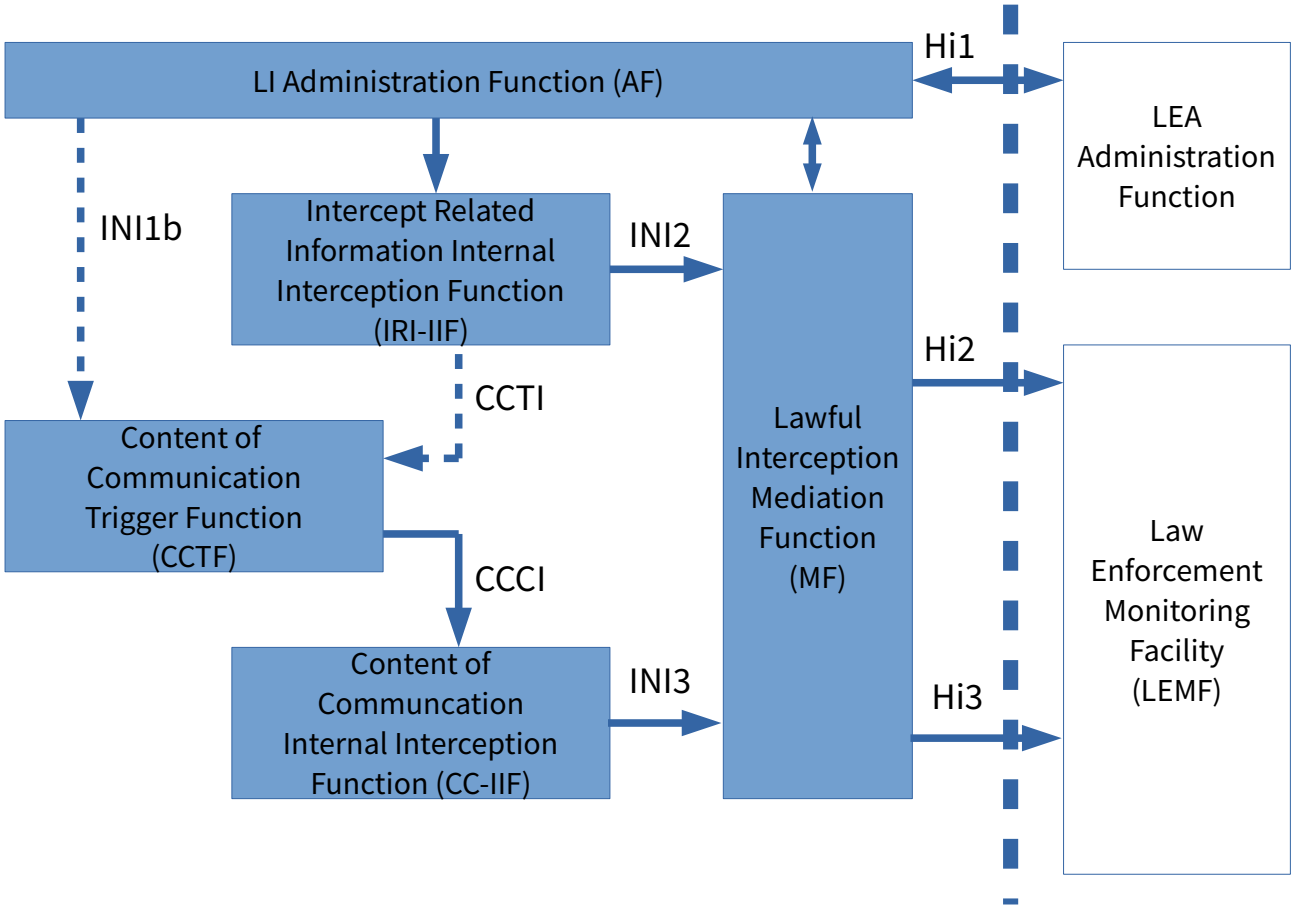
Dokumentiraju se sve opcije, odluke, rasprave

Dokumentacija na EN kako bi se u svakom trenutku mogla predočiti potencijalnim klijentima

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Polazna arhitektura

Krenuli smo od funkcionalne arhitekture predložene u ETSI normama



"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Nadogradnja arhitekture sigurnosnim funkcijama

Referentna arhitektura je bez sigurnosnih elemenata

Nisu definirane sljedeće funkcionalnosti

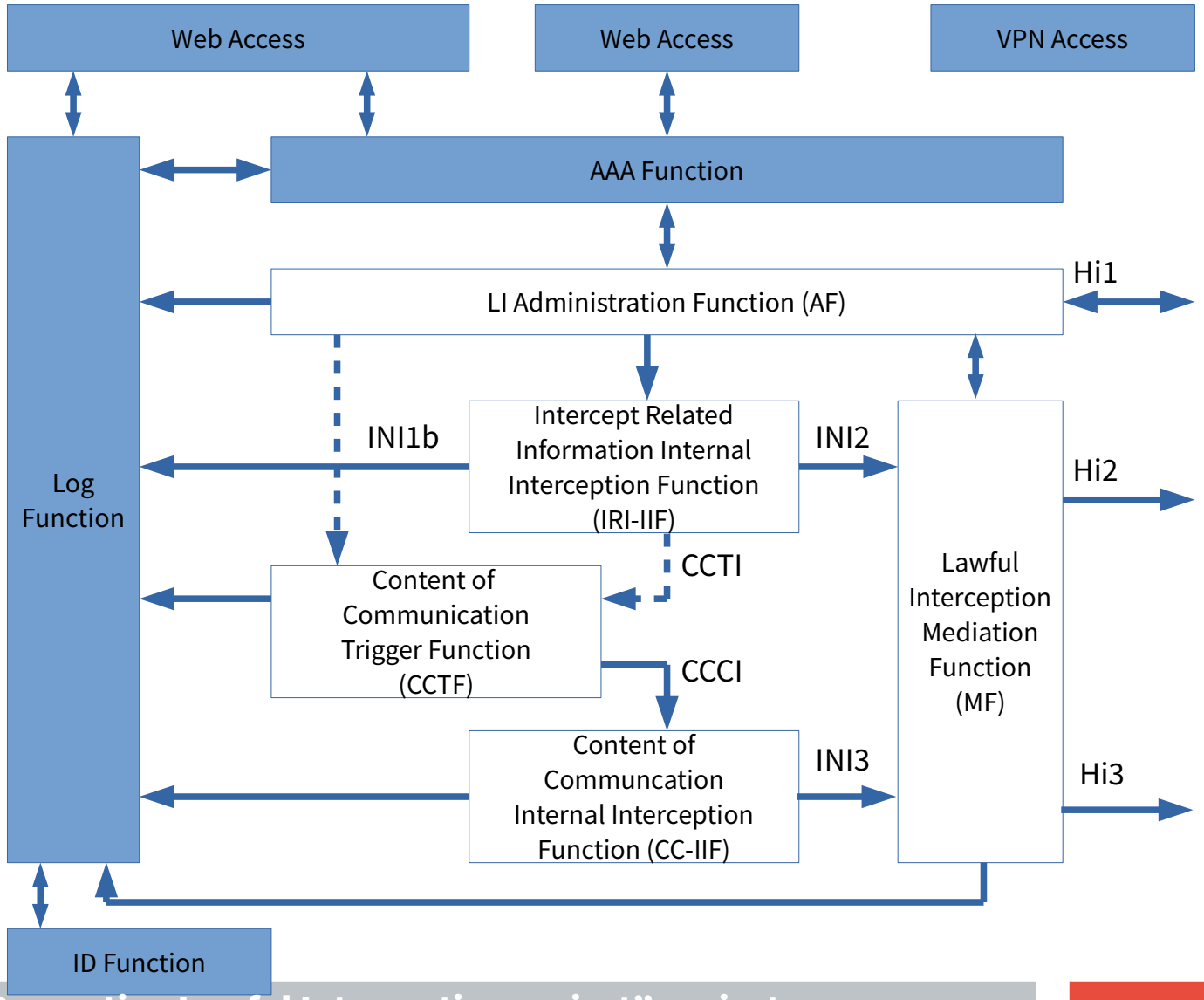
- Autentifikacija i autorizacija – uloge, korisnici, autentifikacija računala i procesa, zaštita komunikacije
- Bilježenje sistemskih i operativnih zapisa
- Sučelje za nadzor i upravljanje
- Ulazna točka u sustav za nadzor pristupa

Dobra sigurnosna praksa je centralizirati te funkcije radi lakšeg održavanja i minimiziranja mogućih pogrešaka

- Ali – istovremeno određene komponente postaju kritičnije u odnosu na druge

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Arhitektura nadograđena sigurnosnim funkcijama



"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Log funkcija

Centralno prikupljanje sistemskih i operativnih zapisa

- Zbog sigurnosti cjelokupnog sustava zapisi se drže na centralnom mjestu
  - Pored toga se zapisi pohranjuju i lokalno na pojedinim komponentama

Omogućava uvid u zapise ovlaštenim korisnicima

- Primjerice
  - Revizori (auditors) – mogu nadgledati aktivnosti drugih uloga (za ono za što su ovlašteni!)
  - Administratori komponenti mogu vidjeti zapise radi pronalaženja pogrešaka
  - Administratori organizacija mogu vidjeti aktivnosti svojih korisnika
- Morali smo definirati sve uloge – što je dio AAA funkcije
- Uloge su definirane na takav način da se spriječi zloupotreba
  - Korisnik – verifikator(i) - revizor(i)

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Model prijetnje

Ne možemo raspravljati o zaštitama dok se ne definira model prijetnje

- Temelj na osnovu kojega se definiraju sigurnosni zahtjevi i razrađuju zaštite
- Definira što se uzima u obzir i što se **ne uzima** u obzir

Temeljni elementi modela prijetnje NGLI sustava

- Najznačajnija prijetnja je sistemski administrator koji se može spojiti na računalo
- Korisnici Web aplikacija nisu prijetnja (Web aplikacija je sigurna)
- Sustav se nalazi u prostorijama nepovjerljive strane koja mu može fizički pristupati po volji

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

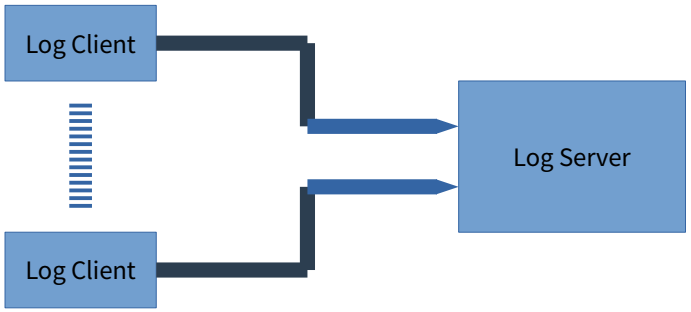
Log sustav

Log funkcija se izvršava na jednom (ili više) poslužitelja

Moraju postojati odgovarajuća komponente (log klijenti) na svim sustavima čiji sistemski i operativni zapisi se bilježe

- Identična komponenta na klijentima se izvršava na svim klijentima
- Pohranjuje log zapise i lokalno

Log sustav sastoji se od *log funkcije* te jednog ili više *log klijenata*

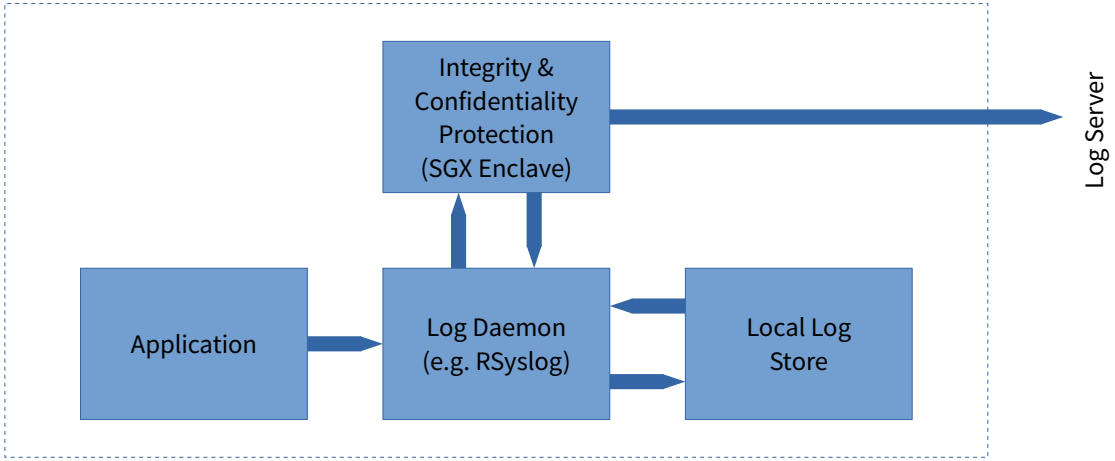


"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Arhitektura Log sustava

Klijenti

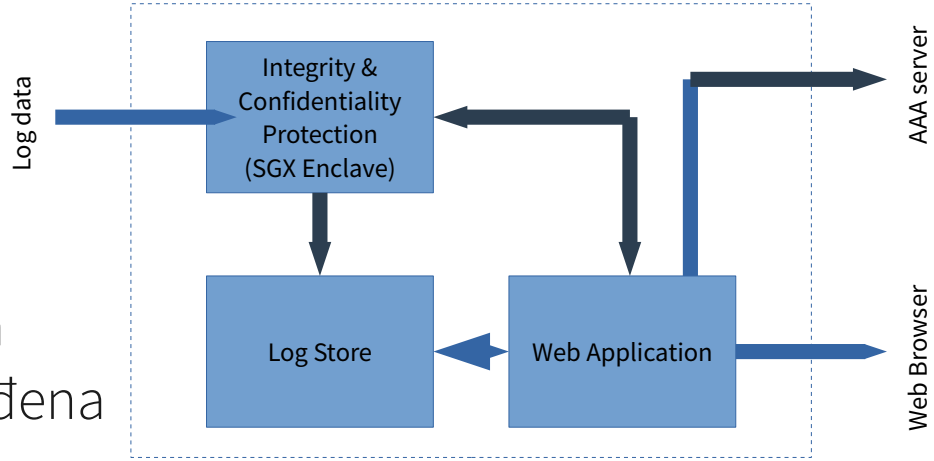
Po svakom računalu ide jedan klijentski sustav bilježenja sistemskih i operativnih zapisa



Poslužitelj

Za sada je samo jedan poslužitelj planiran.

Radi redundancije u budućnosti će arhitektura biti odgovarajuće prilagođena



"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Primjer procedura koje se razrađuju

Enclave, when started, executes the following steps:

1. Enclave loads configuration files from permanent store (disk) and checks their authenticity

2. Enclave generates encryption key, authentication key and their identifiers based on the unique key in the CPU

3. If the key IDs are different than the ones stored on disk then CPU was switched.

4. Enclave tries to connect to database and waits until it can

5. If requested, Enclave checks database authenticity

6. Enclave waits for clients.

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

A što bilježiti?

Vrlo bitno pitanje na koje odgovor treba definirati/tražiti na svakoj razini sustava

Na razini cijelog NGLI sustava smo za sve komponente definirali što bilježe

Dodatno smo analizirali može li se na temelju pohranjenih podataka ispratiti svaka aktivnost na cijelom sustavu

Definiranje formata svih zapisa

Potrebno radi pronalaženja i ispravne zaštite klasificiranih podataka

Prije pohrane u bazu parsiranje elemenata polja

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Sigurnost zapisa

Sigurnost zapisa podrazumijeva njihovu autentičnost i tajnost

- Tajnost je nužna samo za klasificirane podatke
  - Podaci koji na neki način mogu otkriti bilo kakvu informaciju o provođenju nadzora – individualnu ili agregatnu

Autentičnost i tajnost se standardno postižu kriptografskim metodama

- Glavni izazov je upravljanje ključevima

Ključeve je moguće generirati korištenjem ugrađenih ključeva u sve Intelove procesore proizvedene 2015 godine i kasnije

- Pitanje je što sa promjenom računala/CPU-a!?

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Otvorena pitanja

Virtualizacija

VMWare ne podržava virtualizaciju SGX-a (qemu podržava!)

Model prijetnje se donekle mijenja

Spremište log zapisa nije do kraja razrađeno

SQL baza, NoSQL baza, datoteke, …

Pitanje primjenjene šifriranja i (ne)mogućnosti obrade u bazi

Treba načiniti detaljnu analizu pojedinih tehničkih elemenata rješenja

Primjerice, IPC komunikacija unutar OS-a, kako i pod kojim uvijetima se može prisluškivati te manipulirati (MITM napad), sigurnost operacijskog sustava, fizička sigurnost računala

Kako spriječiti programerske pogreške

Primjerice, programer ne zabilježi neki bitan događaj, ili ne zaštiti ispravno klasificiran podatak

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Savjeti za bolju suradnju tvrtka – istraživačka institucija

Komponente su nužne za uspješnu suradnju

- Razumijevanje načina rada i svrhe druge strane!
- Povjerenje
- Dobra komunikacija
- Dobro definiran zajednički cilj
- Posvećenost zajedničkom cilju

Istraživačke institucije – svrha je sticanje (i diseminacija) znanja

- Glavno sredstvo su eksperimenti i prototipi
- Za to je potrebna programska podrška ali nije cilj!

Tvrke – svrha je izrada i prodaja proizvoda (i usluga)

- Glavno sredstvo/alat je znanje, ali to nije cilj!

Kada jedna strana analizira drugu u kontekstu SVOJE svrhe, neumitno dolazi do zaključka da druga strana gubi vrijeme!!!

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Zaključak

Sigurnosni elementi arhitekture su vrlo bitni ali se u funkcionalnim specifikacijama ne spominju

Razvoj sigurnosnih elemenata zahtjeva puno resursa te iskustva

A kao i sve ostalo u vezi sigurnosti – što više očiju, manje sigurnosnih propusta

Suradnja tvrtke SedamIT i FER-a na ovom projektu je pokazni primjer vrlo dobre suradnje

Tvrtka postavlja ograničenja i otvara probleme

FER i tvrtka zajednički pronalaze moguća rješenja

FER radi evaluaciju potencijalnih rješenja sa sigurnosnog stanovišta

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).

Zahvala

This work has been supported by the EU from European regional development fund (ERDF), Operational programme Competitiveness and Cohesion 2014-2020, as part of the "New Generation Lawful Interception project” project no. KK.01.2.1.01.0063 (NG LI).

Kontakti

doc. dr. sc. Stjepan Groš

stjepan.gros@fer.hr, stjepan.gros@icent.hr

www.fer.unizg.hr/stjepan.gros
lisp.fer.unizg.hr
iri-ict.fer.unizg.hr
icent.hr

Laboratorij za informacijsku sigurnost i privatnost
Fakultet elektrotehnike i računarstva
Sveučilište u Zagrebu

Inovacijski centar Nikola Tesla, Zagreb

"New Generation Lawful Interception project" project no. KK.01.2.1.01.0063 (NG LI).