Ministerul Educaţiei, Culturii și Cercetării
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, informatică și microelectronică
Departamentul Ingineria Software și Automatică

RAPORT

Lucrare de Laborator nr.3
Disciplina: Proiectarea sistemelor informaționale
Tema: Familiarizarea cu cerințele notației IDEF0, IDEF3, DFD pentru modelarea și analiza unui proces specific din cadrul sistemului propus pentru dezvoltare

A efectuat: Chirita Stanislav
A verificat: Magdei Octavian

Chișinău 2024

Introducere

Scopul lucrării este de a prezenta un proces selectat din cadrul sistemului propus pentru dezvoltare și de a utiliza standardele de modelare IDEF0, IDEF3 și DFD pentru a analiza și descrie acest proces. Acest laborator are ca obiectiv dezvoltarea abilităților de modelare a proceselor utilizând instrumentele și tehnicile de modelare adecvate, în vederea îmbunătățirii performanței și eficienței sistemului propus.

Importanța modelării proceselor constă în faptul că permite înțelegerea detaliată a fluxurilor de informații și activităților din cadrul unui sistem. Prin aplicarea unor notații standardizate, precum IDEF0, IDEF3 și DFD, este posibil să se obțină o reprezentare clară și coerentă a proceselor, facilitând astfel dezvoltarea, implementarea și optimizarea acestora. Modelarea proceselor ajută la identificarea problemelor și a potențialelor îmbunătățiri, oferind o bază solidă pentru luarea deciziilor și pentru adaptarea sistemului la cerințele utilizatorilor și ale mediului înconjurător.

1. Descrierea procesului ales

Procesul selectat pentru realizarea acestei lucrări de laborator reprezintă **interceptarea și analiza traficului de rețea** într-un sistem integrat. Acest proces este crucial pentru a monitoriza și analiza pachetele de date ce circulă într-o rețea, având ca scop identificarea potențialelor amenințări, detectarea atacurilor și optimizarea performanței rețelei.

În cadrul acestui proces, sistemul va captura, analiza și stoca datele din traficul de rețea pentru a evalua comportamentele și activitățile anormale. Acesta este un instrument important pentru administratorii de rețea, deoarece le permite să monitorizeze constant starea rețelei și să răspundă prompt la orice incident de securitate.

Pașii principali ai procesului includ:

- **Capturarea traficului de rețea**: Acesta este primul pas al procesului, în care pachetele de date sunt interceptate din rețeaua de transmisie. Sistemul va utiliza tehnici de sniffing pentru a prinde pachetele care circulă prin rețea, fie că sunt transmise de calculatoare, servere sau alte dispozitive conectate.
- **Analiza pachetelor capturate**: După capturarea datelor, acestea sunt analizate pentru a identifica informațiile relevante (de exemplu, adrese IP, protocoale de comunicație) și pentru a căuta semne de activitate suspicioasă. Analiza pachetelor poate include inspecția adâncă a pachetelor, pentru a înțelege conținutul acestora și a detecta orice semn de atac sau abuz.
- **Stocarea și procesarea datelor**: Datele capturate și rezultatele analizei sunt stocate pentru o utilizare ulterioară. Aceste date pot fi păstrate în baze de date dedicate, pentru a permite o revizuire ulterioară a traficului și pentru a facilita raportarea sau analiza tendințelor pe termen lung.
- **Detecția și raportarea atacurilor**: Pe baza analizei pachetelor, sistemul va detecta eventuale atacuri cibernetice (cum ar fi atacuri DoS, scanări de porturi, acces neautorizat, etc.). Dacă se identifică un atac, sistemul va trimite un raport către administratorii de rețea, care vor putea să ia măsuri de protecție suplimentare.
- **Revizuirea și ajustarea strategiilor de securitate**: După fiecare incident de securitate sau analiza periodică a rețelei, procesul permite revizuirea și ajustarea strategiilor de protecție. Acest pas poate include modificarea politicilor de securitate ale rețelei, blocarea IP-urilor suspecte sau adaptarea firewall-urilor și a altor instrumente de protecție.
- **Monitorizarea continuă a traficului de rețea**: Pe măsură ce sistemul monitorizează continuu traficul de rețea, va genera notificări și alerte în timp real pentru a informa administratorii despre activitățile neobișnuite sau potențial periculoase.

Procesul de interceptare și analiză a traficului de rețea este esențial pentru menținerea securității în rețelele de calculatoare. Acesta ajută la detectarea rapidă a amenințărilor și la protejarea datelor sensibile împotriva accesului neautorizat, contribuind astfel la stabilitatea și siguranța generală a rețelei.
Acest proces nu doar că protejează infrastructura rețelelor, dar contribuie și la optimizarea utilizării lățimii de bandă și a performanței rețelei, prin identificarea și eliminarea traficului inutil sau abuziv.

2. Elaborarea unui model logic al datelor pentru procesul ales

Obiectivul acestei secțiuni este de a dezvolta și implementa un model logic al datelor pentru **sistemul de interceptare și analiză a traficului de rețea**. Vom folosi notația **IDEF1x** în cadrul aplicației **AllFusion ERwin Data Modeler** pentru a defini structura logică a datelor și a evidenția relațiile esențiale dintre entitățile de date din cadrul acestui proces.

2.1 Diagrama de Context

Diagrama de context reprezintă o viziune de ansamblu a procesului ales pentru analiza și interceptarea traficului de rețea. În cadrul acestui proces, **utilizatorii** trebuie să fie autentificați pentru a putea accesa și interacționa cu sistemul. De asemenea, este necesar să existe un flux constant de **date de rețea** capturate, iar procesul de **analiză a traficului** va fi ghidat de către aplicația informatică.

Fluxul de date va include atât datele brute capturate din rețea, cât și rezultatele procesării și analizei acestora, care vor fi salvate și procesate pentru a detecta eventuale anomalii sau atacuri.

2.2 Diagrama IDEF0

Diagramele IDEF0 sunt utilizate pentru modelarea și analiza funcțiilor unui sistem, în acest caz, pentru a descrie procesul de interceptare și analiză a traficului de rețea.

- **Scopul diagrama IDEF0** este de a oferi o reprezentare vizuală a procesului de **capturare și procesare a pachetelor de rețea**. Acest proces presupune mai mulți pași:
    - **Capturarea pachetelor de rețea**: Fluxul de date provine din rețeaua externă și ajunge la procesul de capturare.
    - **Analiza traficului**: Datele sunt procesate pentru a detecta comportamente anormale.
    - **Stocarea și procesarea rezultatelor**: Rezultatele analizei și datele relevante sunt stocate în baze de date pentru a putea fi accesate ulterior.

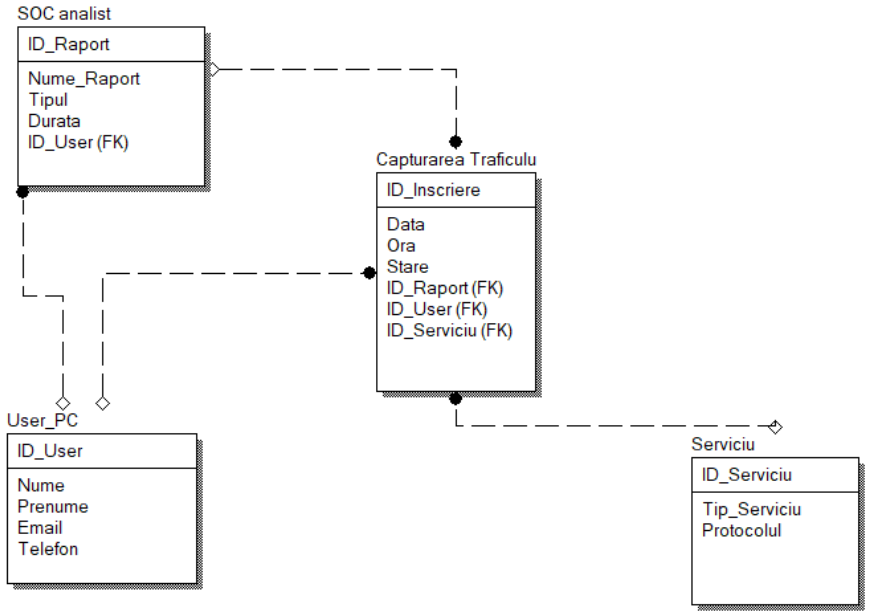

Figura 1 – Diagrama IDEF0

Diagramele IDEF0 vor include și **fluxuri de date** care conectează diferitele procese ale sistemului, ajutând astfel la clarificarea modului în care sunt procesate și transmise informațiile prin sistem.

2.2 Diagrama IDEF3

Diagrama IDEF3 va descrie detaliat fluxurile de date și activitățile legate de **capturarea și analiza traficului de rețea**. În acest caz, procesul de interceptare a pachetelor va fi împărțit în pași specifici:

1. **Verificarea disponibilității traficului de rețea**: În acest pas, se va verifica dacă există trafic de rețea disponibil pentru capturare.
2. **Capturarea pachetelor**: Procesul propriu-zis de capturare a datelor din rețea.
3. **Analiza datelor**: După capturare, datele vor fi analizate pentru a detecta eventuale amenințări, cum ar fi atacuri DoS sau comportamente suspecte.
4. **Generarea rapoartelor**: Rapoartele de analiză vor fi generate și trimise către administratorii de rețea.

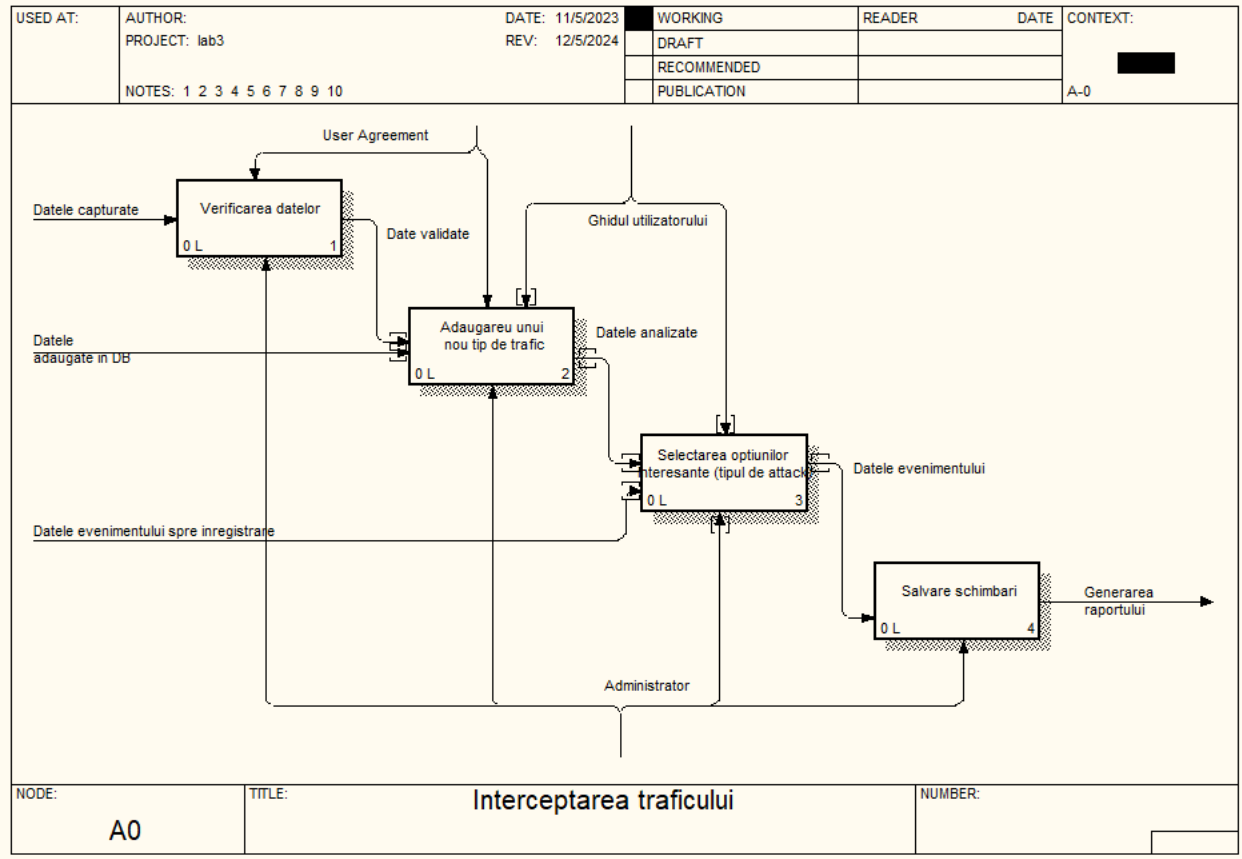

Figura 2 – Diagrama IDEF3

Diagrama IDEF3 va include și decizii, cum ar fi verificarea existenței unor atacuri în rețea, care va determina dacă sunt trimise alerte sau dacă procesul continuă cu analize suplimentare.

2.3 Diagrama DFD

Diagrama Fluxului de Date (DFD) va fi folosită pentru a modela și analiza fluxurile de date dintre procesele sistemului. Această diagramă va include:

- **Procesele**: Capturarea pachetelor de rețea, analiza traficului și generarea rapoartelor.
- **Fluxurile de date**: Care ar putea include datele brute capturate, rezultatele analizei și alertele generate pentru administratorii de rețea.
- **Entitățile externe**: Rețeaua externă care trimite pachetele de date și administratorii care primesc rapoartele.
- **Magazinele de date**: Baza de date de monitorizare unde sunt stocate datele capturate și rezultatele analizei.

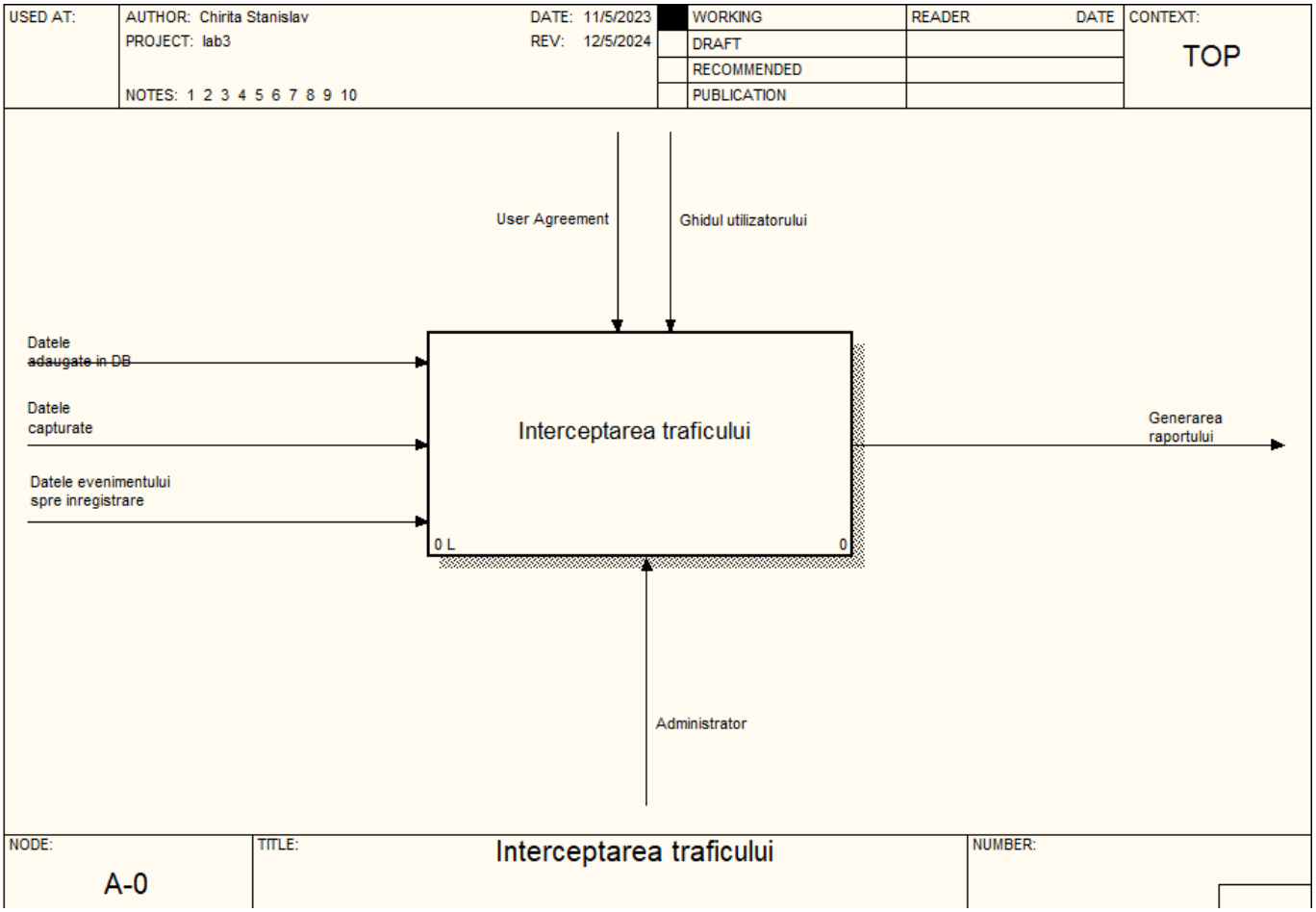

Figura 3 – Diagrama DFD

Diagrama DFD va oferi o viziune clară asupra modului în care datele sunt procesate și cum sunt transmise prin diferitele etape ale sistemului.

Concluzie: Lucrarea de laborator a avut ca obiectiv modelarea și analiza unui proces specific din cadrul unui sistem de interceptare și analiză a traficului de rețea, folosind tehnici standardizate de modelare, precum IDEF0, IDEF3 și DFD. Prin utilizarea acestor tehnici, am reușit să obținem o reprezentare clară și detaliată a funcționării procesului, subliniind pașii implicați, fluxurile de date și interacțiunile dintre componentele sistemului.

În urma modelării, am identificat principalele etape ale procesului: capturarea pachetelor de rețea, analiza acestora pentru detectarea amenințărilor, stocarea și procesarea rezultatelor, generarea rapoartelor și monitorizarea continuă a traficului. Diagramele realizate au contribuit la o înțelegere mai profundă a modului în care informațiile circulă prin sistem și au ajutat la clarificarea rolurilor și responsabilităților fiecărei componente.