“Strategii de detecție a pătrunderilor neautorizate în sisteme informatice”

(Strategies for Intrusion Detection in Computer Systems)

Elaborată de ing. ***Emanuel Ciprian SASU***

REZUMAT

1. Introducere

Teza de doctorat tratează un domeniu de reală actualitate şi anume cel al detecției pătrunderilor neautorizate în rețelele de calculatoare. Una dintre modalitățile concrete prin care un atacator caută să pătrundă într-o rețea de calculatoare, este dată de falsificarea adreselor MAC ale interfețelor plăcilor de rețea. Domeniul este abordat pe larg în literatura de specialitate, fiind prezentate o serie de strategii de detecție și semnalare a cazurilor de pătrundere neautorizată.

Teza aduce contribuții în acest domeniu, prin dezvoltarea unei noi strategii de detecție a pătrunderilor neautorizate, metodă ce are la bază amprentarea stațiilor din rețea pe baza traficului constant generat de acestea în rețea, către anumite destinații IP. Publicațiile științifice susțin actualitatea cercetărilor întreprinse ale autorului, referitoare la subiectul propus.

2. Structurarea şi conținutul tezei

Capitolul 1 este intitulat „Introducere”, şi debutează cu prezentarea oportunității şi a obiectivelor tezei. Într-un context în care rețelele de calculatoare sunt utilizate pe scară largă în prezent, problemele de securitate sunt frecvente şi

necesită o abordare corespunzătoare, care să limiteze efectele negative şi să ofere siguranță şi fiabilitate.

Identificarea fiecărei stații dintr-o rețea de calculatoare se poate pe baza adresei fizice a plăcii de rețea (adresa MAC). Una dintre problemele de securitate este legată de pătrunderea neautorizată a unui utilizator într-o rețea de calculatoare, prin folosirea de către atacator a unei adrese MAC autorizate, astfel încât să pară a fi o stație autorizată.

Oportunitatea tezei este definită în acest context, având următoarele obiective propuse:

- evaluarea stadiului actual, pentru determinarea gradului de acoperire pe care metodele folosite în prezent pentru detectarea adreselor MAC falsificate, îl au în contextul unor probleme concrete apărute în practică;
- dezvoltarea unei metode noi de detecție a falsificării adreselor MAC, metodă care se foloseşte de o amprentă de trafic cu ajutorul căreia validează sau invalidează identitatea unei adrese MAC;
- modelarea, implementarea şi analizarea fiabilității sistemului de detecție propus;
- implementarea unui mediu de simulare adecvat

Capitolul 2 este intitulat "Securizarea rețelelor de calculatoare împotriva pătrunderilor neautorizate", şi prezintă necesitatea securizării rețelelor de calculatoare în contextul frecventelor atacuri cibernetice, precum şi principalele strategii folosite în prezent pentru detectarea încercărilor de pătrundere neautorizată prin falsificarea adreselor MAC.

Prima categorie de strategii abordează problema prin prisma analizării unor parametrii care intră în componența pachetelor de rețea, cum ar fi:

- verificarea ID-ului de VLAN
- verificarea numărului de secvență şi a parametrului „interarrival time"

- verificarea parametrului „hop-count”

Fiecare strategie este descrisă pe larg, prezentându-se domeniul de aplicabilitate și avantajele pe care le conferă.

A doua categorie se aplică în mod direct echipamentelor wireless, și abordează falsificarea adreselor MAC printr-o amprentare a echipamentului wireless și compararea amprentei stabilite inițial, cu amprenta actuală. Astfel se pot aminti următoarele strategii:

- verificarea răspunsului echipamentelor wireless la mesaje deformate;
- verificarea distribuției cadrelor de tip „frame-request”;
- verificarea intensității semnalului recepționat;
- verificarea parametrului „clock-skew”

Ultima parte a capitolului realizează o analiză critică a metodelor prezentate, prin prisma aplicabilității acestora în diverse situații specifice.

În Capitolul 3, “Detecția adreselor MAC falsificate prin metoda Destination Traffic Fingerprint”, se prezintă contribuțiile autorului tezei în domeniul abordat, prin dezvoltarea unei noi strategii de detecție a falsificării adreselor MAC.

În prima parte a capitolului se realizează o descriere generală a metodei “Destination Traffic Fingerprint” (DTF), pornind de la elementele care stau la baza dezvoltării metodei.

Metoda DTF identifică o stație pe baza unei amprente de trafic, care are în componența sa destinații IP cu care stația comunică în mod constant, împreună cu procentele de prezență cu care aceste destinații se regăsesc în traficul stației, într-o evaluare realizată la nivel de minut.

Determinarea traficului constant este prezentată succint, și este urmată de o modelare sistemică ce descrie toate fazele necesare extragerii amprentei de referință și validării adreselor MAC întâlnite în trafic. Fiecare subsistem este

descris prin mărimile de intrare și ieșire, oferind astfel o imagine concludentă asupra operațiilor realizate.

Traficul generat de o stație către o anumită adresă IP, poate fi considerat ca făcând parte din următoarele categorii:

- ***trafic constant*** – un transfer de date între o stație din rețea şi o destinație IP, care, fiind monitorizat la nivel de minut pentru o perioadă lungă de timp, prezintă o frecvență relativ constantă a minutelor în care sursa a trimis pachete de date spre destinația IP pe întreaga perioadă evaluată;
- ***trafic temporar*** - un transfer de date între o stație din rețea şi o destinație IP, care, fiind monitorizat la nivel de minut pentru o perioadă lungă de timp, prezintă o frecvență relativ constantă a minutelor în care sursa a trimis pachete de date spre destinația IP doar pe anumite subintervale de timp din întregul interval evaluat;
- ***trafic punctual*** - un transfer de date între o stație din rețea şi o destinație IP, care, fiind monitorizat la nivel de minut pentru o perioadă lungă de timp, prezintă o frecvență relativ constantă a minutelor în care sursa a trimis pachete de date spre destinația IP repartizate aleatoriu şi izolat pe axa timpului, pe durata intervalului de timp evaluat;

Pentru a determina traficul constant, s-au definit următorii parametrii:

- ***procentul de prezență*** – definit ca fiind raportul dintre numărul de minute în care există trafic către o destinație anume, şi numărul total de minute aferente perioadei evaluate,
- ***procentul de absență maximă*** – definit ca raport dintre numărul maxim de minute consecutive în care nu a avut loc trafic către o destinație, şi numărul total de minute evaluate;

- ***criteriul de prezență pe subintervale egale*** – împarte intervalul evaluat într-un număr dat de subintervale egale, şi varifică prezența traficului în toate aceste subintervale
- ***puterea amprentei de referință*** – oferă o măsură de evaluare a stabilității, credibilității şi vitezei de validare a sistemului.

Modelarea sistemică a determinării amprentei de referință este prezentată în Fig. 1. Fiecare subansamblu este caracterizat de mărimile de intrare-ieşire astfel:

- *intrarea şi ieşirea sistemului:*

$$u(t)=M_{NP}\{NP_k|k-variabil\ ,\ functie\ de\ t\},\ M_{NP}\subset M_{IP}. \quad (1)$$

$$y(t)=M_{DTF}\{P(IP_k\ ,\ PP_k)|IP_k-destinație\ cu\ trafic\ constant\ PP_k\} \quad (2)$$

- *Subsistemul „FILTRU MAC”:*

$$u_1(t)=u(t)=M_{NP}\{NP_k|k-variabil\ ,\ functie\ de\ t\},\ M_{NP}\subset M_{IP}. \quad (3)$$

$$y_1(t)=M_{NPM}\{NP_{kM}|MAC_k=MAC\},\ M_{NPM}\subset M_{NP}\subset M_{IP}. \quad (4)$$

- *Subsistemul „LISTA IP”:*

$$u_2(t)=y_1(t)=M_{NPM}\{NP_{kM}|MAC_k=MAC\},\ M_{NPM}\subset M_{NP}\subset M_{IP}. \quad (5)$$

$$y_2(t)=M_2\{IP_k|\forall\ NP_{kM}\in M_{NPM}\ ,\ IP_k=adresa\ IP\ destinatie\ din\ NP_{kM}\} \quad (6)$$

- *Subsistemul „SUMATOR IP”:*

$$u_3(t)=y_2(t)=M_2\{IP_k|\forall\ NP_{kM}\in M_{NPM}\ ,\ IP_k=adr.\ IP\ dest.\ din\ NP_{kM}\} \quad (7)$$

$$y_3(t)=y_2(t-1)+u_3(t)=M_3\{a_k\ IP_k|a_k-numar\ de\ aparitii\ a\ lui\ IP_k\} \quad (8)$$

- *Subsistemul „CALCUL PREZENȚĂ”*

$$u_4(t)=y_3(t)=M_3\{a_k\ IP_k|a_k-numar\ de\ aparitii\ a\ lui\ IP_k\} \quad (9)$$

$$y_4(t)=M_4\{P(IP_k\ ,PP_k)|PP_k=\frac{a_k}{t}\} \quad (10)$$

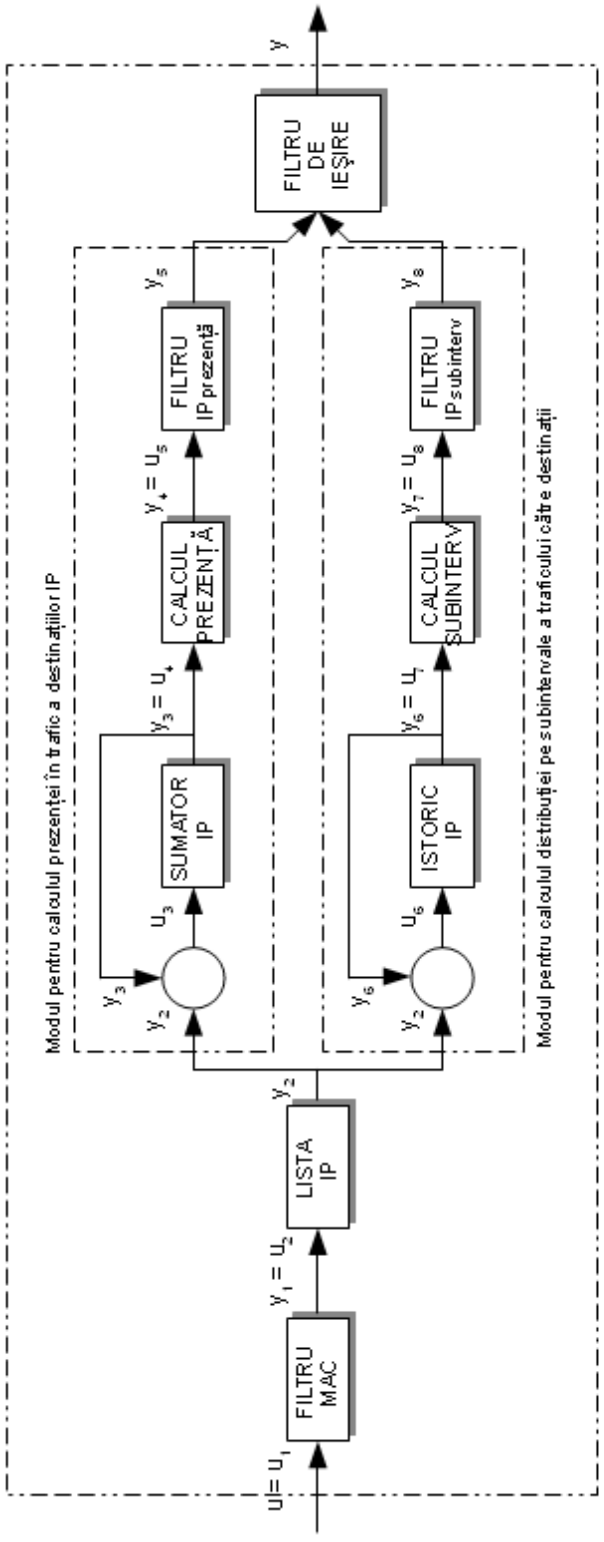

Figura 1 – Schema bloc a sistemului destinat determinării amprentei de trafic, prin metoda DTF

- *Subsistemul „FILTRU IPprezență”:*

$$u_5(t)=y_4(t)=M_4\{P(IP_k, PP_k)|PP_k=\frac{a_k}{t}\} \quad (11)$$

$$y_5(t)=M_5\{P(IP_k, PP_k)|P(IP_k, PP_k)\in M_4 si\ PP_k \geq LP\} \quad (12)$$

- *Subsistemul „ISTORIC IP”:*

$$u_6(t)=y_2(t)=M_2\{IP_k|\forall\ NP_{kM}\in M_{NPM}, IP_k=adr.\ IP\ dest.\ din\ NP_{kM}\} \quad (13)$$

$$y_6(t)=M_6\{P(IP_k, M_{ISTORIC})|M_{ISTORIC}=\{t_k|t_k-min.\ cu\ trafic\ catre\ IP_k\} \quad (14)$$

- *Subsistemul „CALCUL SUBINTERVALE”:*

$$u_7(t)=y_6(t)=M_6\{P(IP_k, M_{ISTORIC})|M_{ISTORIC}=\{t_k|t_k-min.trafic\}\} \quad (15)$$

$$y_7(t)=M_7\{P(IP_k, NSI_k)|NSI_k-nr\ de\ subinterv.\ pentru\ IP_k, 0\leq NSI_k \quad (16)$$

- *Subsistemul „IPsubinterval”:*

$$u_8(t)=y_7(t)=M_7\{P(IP_k, NSI_k)|NSI_k-nr\ subinterv.\ pt.\ IP_k, 0\leq NSI_k \quad (17)$$

$$y_8(t)=M_8\{P(IP_k, NSI_k)|NSI_k\in M_7 si\ NSI_k\geq MIN_{INTERV}\} \quad (18)$$

- *Susbsistemul „FILTRU DE IEŞIRE”:*

$$u_9(t)=y_5(t)\ si\ y_8(t) \quad (19)$$

$$y(t)=y_9(t)=y_5(t)\cap y_8(t)=M_{DTF}\{P(IP_k, PP_k)|IP_k\in M_5 si\ IP_k\in M_8\} \quad (20)$$

În acest context, se defineşte Gradul Global de Recunoaştere ca fiind raportul dintre suma gradelor individuale de recunoaştere RDi a fiecărei destinații IP ce intră în componența amprentei de referință, şi numărul total de destinații din cadrul amprentei de referință:

$$ODR_{standard}=\frac{\sum_{i=1}^{TDIP_{ref}} RD_i}{TDIP_{ref}} \quad (21)$$

Calculul gradului de recunoaştere a unei destinații se poate realiza în manieră standard, sau în manieră ponderată, ținând cont de ponderea cu care destinația IP intră în cadrul amprentei de referință

Capitolul 4 este intitulat “Toolbox software pentru studiul metodei DTF” şi prezintă un pachet de aplicații software realizate de către autor cu scopul de a integra aspectele teoretice, într-un sistem practic, care să permită detecția adreselor MAC falsificate.

Aplicația software “Packet Recorder” permite captarea pachetelor de date din rețea și stocarea informațiilor într-o structură care să permită ulterior amprentarea stațiilor.

Aplicația software “Network Detector” reprezintă un mediu adecvat de analiză și simulare, fiind alcătuit dintr-o serie de module care oferă cadrul necesar studiului în cadrul metodei DTF. Modulul de simulare permite realizarea unei rețele formate din datele extrase de către “Packet Recorder” și observarea practică a modului de funcționare a metodei DTF.

În Capitolul 5 – “Rezultate experimentale”, se prezintă rezultatele experimentale obținute prin aplicarea metodei DTF pe un număr vast de calculatoare, cu scopul de a dovedi faptul că se pot genera amprente de referință pe baza traficului constant pe care stațiile îl au cu diverse destinații IP.

În urma experimentelor realizate, rezultatele obținute au confirmat faptul că pe durate lungi de timp, stațiile comunică în rețea în mod constant cu anumite destinații IP. Includerea acestor destinații în amprentele de referință, va conduce la o corectă validare a adreselor MAC în traficul monitorizat.

La final, Capitolul 6 concluzionează demersul ştiinţific întreprins prin cercetările din teză, focalizându-se pe concluziile şi contribuțiile aduse. Sunt prezentate de asemenea tendințele de cercetare viitoare.

3. Contribuții originale

Contribuțiile autorului în domeniul actual al problematicii detecției adreselor MAC falsificate, sunt demne de remarcat, fiind concretizate prin soluții teoretice şi practice.

Activitatea de doctorat a fost judițios coroborată cu elaborarea a 7 publicații în nume propriu sau în colectiv, în domeniul abordat în teză. Astfel, principalele rezultate obținute au fost publicate după cum urmează: trei sunt indexate in volumele unor manifestări ştiințifice (Proceedings) cotate ISI, iar patru sunt indexate în baze de date BDI.

Pornind de la obiectivele declarate ale tezei prezint în continuare o selecție a celor mai importante contribuții:

- realizarea unei analize sistemice a detecției adreselor MAC falsificate;
- realizarea unui studiu critic al metodelor de detecție actuale, prin prisma răspunsului pe care acestea îl au în diverse situații specifice;
- dezvoltarea unei metode noi de detecție a adreselor MAC falsificate, numită "*Destination Traffic Fingerprint*" (DTF), pe baza unei amprente de trafic alcătuite din destinațiile IP cu care stația comunică în mod constant;
- definirea matematică a termenilor și parametrilor care caracterizează metoda DTF;
- dezvoltarea unui model sistemic pentru determinarea amprentei de referință a unei stații, și respectiv unui model sistemic destinat validării adresei MAC, ambele prezentând detaliat formalismele componente;
- realizarea unui pachet de aplicații software necesare studiului metodei DTF;

- realizarea unui experiment care validează amprentarea pe baza traficului constant.

4. Concluzii finale

Teza elaborată de autor reprezintă o lucrare ştiinţifică importantă, care tratează probleme atât teoretice cât şi practice în domeniul detecției pătrunderilor neautorizate prin falsificarea adreselor MAC.

Teza este structuraă corespunzător și cuprinde un material bogat, explicat detaliat, fapt ce ajută la o înțelegere mai bună a conceptelor prezentate şi a analizei rezultatelor obținute. Este de subliniat preocuparea pentru claritatea expunerii şi fundamentarea corectă a soluțiilor propuse.