Universitatea POLITEHNICA din București

Facultatea de Automatică și Calculatoare,
Departamentul de Calculatoare

TEZĂ DE DOCTORAT

REZUMAT

Îmbunătățirea percepției aplicațiilor prin firewalling distribuit

Conducător Științific:
Prof. Dr. Ing. Nicolae Țăpuș

Autor:
Ing. Radu-Alexandru Mantu

București, 2025

În primele zile ale internetului, amenințările externe la adresa rețelei erau ușor de contracarat datorită naturii clare a clienților, precum și disponibilității limitate a aplicațiilor web. Asocierea dintre numerele porturilor serverului și aplicațiile care ascultau putea fi stabilită mai fiabil. La rândul său, acest lucru simplifica evaluarea scopului fiecărei noi conexiuni. Cu toate acestea, în 2003, Gartner Research a definit ceea ce considera a fi patru abordări pentru securitatea gateway-urilor, introducând astfel termenul „Next Generation Firewall" (NGFW). Cu scopul de a combate amenințările emergente la adresa securității rețelei, NGFW-urile au integrat sisteme de detectare și prevenire a intruziunilor (IDS/IPS) și conștientizarea aplicațiilor în firewall-urile convenționale. Chiar și în acea perioadă, se putea afirma că aplicațiile de la nivelul endpoint-urilor erau, în mare parte, detașate de semnificația pe care o conferea portul la care erau asociate. Astfel, tehnici precum JA3 sau Amprentarea cu Lanțuri Markov au fost dezvoltate ulterior în scopul mitigării active a amenințărilor. Totuși, eficacitatea lor (precum și cea a IDS/IPS) este semnificativ redusă atunci când sunt aplicate traficului criptat. În ciuda eforturilor continue pentru clasificarea traficului criptat, decriptarea traficului TLS rămâne, fără îndoială, soluția cea mai predominantă pentru această problemă, implicând un compromis între confidențialitatea utilizatorului și securitatea generală a rețelei.

În ciuda acestei deficiențe, firewall-urile de generație următoare (NGFW) sunt mai relevante ca niciodată datorită adoptării continue a arhitecturilor de rețea Zero Trust. Pe măsură ce întreprinderile încearcă să implementeze politici de acces la resurse din ce in ce mai detaliate, bazate pe principiul privilegiului minim, utilizarea micro-segmentării a devenit din ce în ce mai frecventă. Acest lucru reiese și din rapoartele companiei Alphabet (i.e., Google) privind tranziția către paradigma Zero Trust, adică Google BeyondCorp. Susținem că sistemele actuale de decizie privind accesul, care se bazează în mod obișnuit pe autentificarea utilizatorului, sunt insuficiente pentru prevenirea atacurilor facilitate de versiuni vulnerabile ale uneltelor comune sau bibliotecilor partajate. De exemplu, recentul backdoor `liblzma` sau atacurile asupra lanțurilor de aprovizionare software. Această problemă este agravată și mai mult de fluidizarea crescândă a demarcațiilor rețelei, un fenomen determinat de necesitatea mișcării libere între rețelele deținute de întreprinderi și rețelele publice. Considerăm că abordarea acestor provocări ar trebui să fie sprijinită de dispozitivele utilizatorilor finali.

Contribuțiile Tezei

În această teză, oferim o soluție cuprinzătoare pentru conștientizarea aplicațiilor sub forma unui firewall distribuit. Acest firewall a fost implementat de la zero și are două implementări alternative, mai limitate în scop, dar care servesc drept proof-of-concept pentru direcții viitoare de cercetare. În plus, propunem o metodă de adnotare a pachetelor care permite firewall-ului nostru să transmită o dovadă de conformitate pentru traficul emis către alte instanțe ale aceluiași firewall. Acestă dovadă poate fi verificată de IDS/IPS-uri sau firewall-uri software existente.

Contribuțiile aduse sunt următoarele:

1. **Evaluarea acceptării opțiunilor de protocol în Internet:** Prin implementarea unui instrument de adnotare a traficului cu opțiuni IP, TCP și UDP, realizăm teste de accesibilitate între 21 de locații din întreaga lume, patru furnizori de cloud și universitatea noastră.

2. **Implementarea unui firewall distribuit conștient de aplicații** Oferim mai multe variante ale acestui firewall. Versiunea principală este dezvoltată pentru Linux și funcționează strict în spațiul utilizator. O alternativă implementată ca modul de kernel oferă mai puține funcționalități, dar demonstrează o creștere semnificativă a performanței. A treia variantă reprezintă o implementare proof-of-concept pentru sistemele Windows.

3. **Evaluarea în medii realiste:** Testăm implementările firewall-ului bazat pe Linux atât în medii de centre de date, pe servere cu NIC-uri de 10Gbps, cât și în medii de tip desktop, pe sisteme Intel NUC cu NIC-uri de 1Gbps. Oferim utilizatorului opțiunea de a ajusta firewall-ul și de a selecta ce compromisuri de securitate sunt acceptabile pentru a crește performanța.

4. **Metodă de adnotare a pachetelor și verificare a conformității:** Propunem o schemă de adnotare a pachetelor bazată pe opțiuni de protocol. Deși am decis în cele din urmă să utilizăm opțiunile IP ca mod de transer a dovezii de conformitate atașată fiecărui pachet, discutăm limitările actuale ale opțiunilor TCP și UDP care ne-au împiedicat să adoptăm o alternativă la nivelul 4 a stivei OSI. În acest context, discutăm și eforturile curente ale grupurilor de lucru din IETF pentru a remedia neajunsurile opțiunilor TCP și UDP.

5. **Soluții de integrare în rețea:** Pentru a integra schema noastră de adnotare a pachetelor în rețelele existente fără a fi necesară implementarea firewall-ului pe mai multe gazde decât este necesar, am dezvoltat module pentru `iptables` și `snort3` capabile să verifice dovada de conformitate atașată fiecărui pachet.

6. **Prezentare generală a stadiului actual în fuzzing-ul aplicațiilor de rețea:** Explorăm posibilitatea de a utiliza fuzzing-ul ca o măsură suplimentară pentru asigurarea securității aplicațiilor pe care le includem în politicile noastre de tip whitelist pentru firewall.