Tehnologii Multicore pentru Paralelizarea Procesului de Detecție și Prevenție a Intruziunilor la Nivel de Rețea

Amenințările cibernetice din ultimul deceniu au influenţat modul în care industria de securitate software a evoluat. Odată cu creşterea nivelului de interconectare a utilizatorilor obişnuiţi şi a companiilor, suprafaţa de atac vulnerabilă a crescut. Această teză îşi propune să analizeze elementele care guvernează deciziile de dezvoltare a noilor generaţii de soluţii de securitate şi să propună noi mecanisme prin care să îmbunătăţească performanţa lor. Problema securităţii va fi tratată în special din perspectiva securizării comunicaţiei la nivel de reţea, iar metodele de îmbunatăţire se vor baza noile trenduri în materie de tehnologii software şi hardware. Teza abordează problemele de performanţă computaţionale întâlnite în soluțiile de securitate prin paralelism.

Teza debutează cu o imagine a domeniului securităţii cibernetice şi a ameninţărilor cu care se confruntă utilizatorii şi analiştii de reţea, şi metodologiile folosite pentru evaluarea soluţiilor propuse. Cercetarea tratează problema optimizării soluțiilor de detecţie a intruziunii din diferite perspective ale paralelismului. Direcţia principală este dată de folosirea procesoarelor paralele şi a GPU-urilor în securitatea reţelelor. Optimizarea NIDPS-urilor (*network intrusion detection and prevention system*) este definită ca îmbunătăţirea nivelului de securitate oferit, accelerarea vitezei de execuţie şi reducerea consumului de resurse.

Pentru a identifica zone ce pot fi îmbunătăţite, teza realizează un studiu al soluţiilor open source existente în materie de detecţie a intruziunilor la nivel de reţea. O concluzie a analizei de performanţă este că algoritmii de căutare a şirurilor joacă un rol foarte important în procesele de detecţie a intruziunilor (fie că e vorba de scanare de fişiere de pe disk sau a traficului din reţea). O serie de experimente folosind OpenCL şi fire de execuţie pe CPU sunt folosite pentru a compara performanţele unor algoritmi de căutare de şiruri pe sisteme desktop şi embedded.

Teza discută impactul paralelismului la nivel instrucţiune asupra diferitelor elemente din stiva software a unui sistem de securitate: funcţii de dispersie, criptare, căutare şiruri, etc. Sunt discutate tehnologiile existente şi oportunitatea folosirii lor pe anumite dispozitive cu baterie.

Învăţarea automată este abordată în contextul securităţii reţelelor. Marele avantaj adus de învăţarea automată în securitate este legat de identificarea noilor ameninţări. Industria de securitate se bazează deja pe colectarea unor cantităţi mari de date sub formă de baze de date malware, statistici ale traficului de reţea, jurnale, capturi, etc. Pe măsură ce ameninţările evoluează dincolo de capabilităţile de detectare ale aplicaţiilor tradiţionale, nevoia de găsi o structură în ceea ce pare a fi haos creşte. Teza prezintă o serie de experimente ce îşi propun să îmbunătăţească performanţele prelucrării de date, antrenării şi lansării modelelor de învăţare automată.

În concluzie, paralelismul este o temă de actualitate atât în securitatea reţelelor cât şi în alte domenii din ştiinţa calculatoarelor. În prezent, metodele folosite de NIDPS se pretează acestui tip de optimizare. Pe măsură ce tehnologiile hardware şi API-urile de procesare paralelă evoluează, apar noi oportunităţi de accelerare a procesului de detecţie de malware şi al intruziunilor la nivel de reţea. Folosirea colaborativă a CPU-ului şi GPU-ului pentru a rezolva probleme de securitate poate mări gradul de adoptare şi performanţa soluţiilor existente.