O introducere în sistemele de detectare a intruziunilor

Hervé Debar
IBM Research, Laboratorul de Cercetare din Zurich,
S¨aumerstrasse 4, CH–8803 R¨uschlikon, Elveția deb@zurich.ibm.com

Abstract

Sistemele de detectare a intruziunilor vizează detectarea atacurilor împotriva sistemelor și rețelelor informatice sau, în general, împotriva sistemelor informaționale. Într-adevăr, este dificil să se furnizeze sisteme de informații sigure și să le mențină într-o astfel de stare sigură pe durata vieții și utilizării lor. Uneori, moștenirea sau constrângerile operaționale nici măcar nu permit definirea unui sistem informațional complet securizat.
Prin urmare, sistemele de detectare a intruziunilor au sarcina de a monitoriza utilizarea unor astfel de sisteme pentru a detecta orice apariție a stărilor nesigure. Ei detectează încercările și utilizarea greșită activă fie de către utilizatorii legitimi ai sistemelor informatice, fie de către părți externe pentru a abuza de privilegiile lor sau a exploata vulnerabilitățile de securitate.
Această lucrare este prima dintr-o serie de două părți; introduce conceptele utilizate în sistemele de detectare a intruziunilor în jurul unei taxonomii.

1 Introducere

De la lucrarea fundamentală a lui Denning în 1981 [11], au fost create multe prototipuri de detectare a intruziunilor.
Sobirey menține o listă parțială de 59 dintre ele [52]. Sistemele de detectare a intruziunilor au apărut în zona securității computerelor din cauza dificultății de a se asigura că un sistem informatic va fi lipsit de defecte de securitate.
Într-adevăr, o taxonomie a defectelor de securitate de Landwehr et al. [36] arată că sistemele informatice suferă de vulnerabilități de securitate, indiferent de scopul, producătorul sau originea lor și că este dificil din punct de vedere tehnic, precum și costisitor din punct de vedere economic (atât în ceea ce privește construirea, cât și întreținerea unui astfel de sistem) să se asigure că sistemele și rețelele informatice nu sunt susceptibile la atacuri.

2 Descrierea unui sistem generic de detectare a intruziunilor

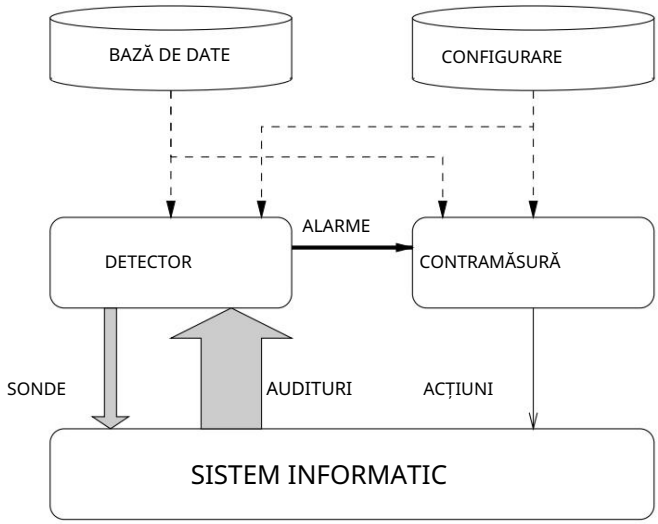
2.1 Terminologie

Termenul de sistem (alias sistem țintă) este folosit aici pentru a desemna sistemul de informații monitorizat de sistemul de detectare a intruziunilor. Poate fi o stație de lucru, un element de rețea, un server, un mainframe, un firewall, un server web etc.

Termenul de audit denotă informațiile furnizate de un sistem cu privire la funcționarea și comportamentul său interioară. Exemplele de audituri includ, dar nu se limitează la, pista de audit C2, contabilitate și syslog în lumea UNIX, Syslog în lumea MVS, jurnalul de evenimente în Windows NT și biletele de incident în rețelele X25. O descriere a unora dintre aceste audituri este dată în Secțiunea 5.

2.2 Descriere

Un sistem de detectare a intruziunilor dobândește informații despre un sistem informațional pentru a realiza o diagnoză asupra stării de securitate a acestuia din urmă. Scopul este de a descoperi breșe de securitate, tentative de încălcare sau vulnerabilități deschise care ar putea duce la posibile încălcări. Un sistem tipic de detectare a intruziunilor este prezentat în Figura 1.



NOTĂ: Grosimea săgeții reprezintă cantitatea de informații care curge de la o componentă la alta.

Figura 1: Sistem foarte simplu de detectare a intruziunilor.

Un sistem de detectare a intruziunilor poate fi descris la un nivel foarte macroscopic ca un detector care prelucrează informațiile care provin din sistemul de protejat (Fig. 1). Acest detector poate lansa, de asemenea, sonde pentru a declanșa procesul de audit, cum ar fi solicitarea numerelor de versiune pentru aplicații. Folosește trei tipuri de informații: informații pe termen lung legate de tehnica utilizată pentru a detecta intruziunile (o bază de cunoștințe a atacurilor, de exemplu), informații de configurare despre starea curentă a sistemului și informații de audit care descriu evenimentele care au loc pe sistem.

Rolul detectorului este de a elimina informațiile inutile din pista de audit. Apoi prezintă fie o vedere sintetică a acțiunilor legate de securitate întreprinse în timpul utilizării normale a sistemului, fie o vedere sintetică a stării curente de securitate a sistemului. Se ia apoi o decizie pentru a evalua probabilitatea ca aceste acțiuni sau această stare să poată fi considerate simptome ale unei intruziuni sau vulnerabilități. O componentă de contramăsuri poate lua apoi acțiuni corective fie pentru a preveni executarea acțiunilor, fie pentru a schimba starea sistemului la o stare sigură.

2.3 Eficiența sistemelor de detectare a intruziunilor

Pentru a evalua eficiența unui sistem de detectare a intruziunilor, Porras și Valdes [42] au propus următorii trei parametri:

Precizie. Precizia se ocupă de detectarea corectă a atacurilor și de absența alarmelor false. Inexactitatea apare atunci când un sistem de detectare a intruziunilor semnalează o acțiune legitimă în mediu ca anormală sau intruzivă.

Performan ă. Performanța unui sistem de detectare a intruziunilor este rata la care sunt procesate evenimentele de audit. Dacă performanța sistemului de detectare a intruziunilor este slabă, atunci detectarea în timp real nu este posibilă.

Completitudine. Completitudinea este proprietatea unui sistem de detectare a intruziunilor de a detecta toate atacurile. Incompletitudinea apare atunci când sistemul de detectare a intruziunilor nu reușește să detecteze un atac. Această măsură este mult mai greu de evaluat decât celelalte deoarece este imposibil să aveți o cunoaștere globală despre atacuri sau abuzuri de privilegii.

Să introducem două proprietăți suplimentare:

Toleranță la erori. Un sistem de detectare a intruziunilor ar trebui să fie el însuși rezistent la atacuri, în special la atacurile de tip denial-of-service, și ar trebui proiectat având în vedere acest scop. Acest lucru este deosebit de important deoarece majoritatea sistemelor de detectare a intruziunilor rulează deasupra sistemelor de operare sau hardware-ului disponibile comercial, despre care se știe că sunt vulnerabile la atacuri.

Promptitudine. Un sistem de detectare a intruziunilor trebuie să efectueze și să-și propage analiza cât mai repede posibil pentru a permite ofițerului de securitate să reacționeze înainte de a fi provocat multe daune și, de asemenea, pentru a preveni atacatorul să submina sursa de audit sau sistemul de detectare a intruziunilor însuși. Aceasta implică mai mult decât măsura performanței, deoarece nu cuprinde doar viteza intrinsecă de procesare a sistemului de detectare a intruziunilor, ci și timpul necesar pentru a propaga informația și a reacționa la ea.

3 elemente de taxonomie

Introducem trei concepte de clasificare a sistemelor de detectare a intruziunilor, care sunt rezumate în Fig. 2.

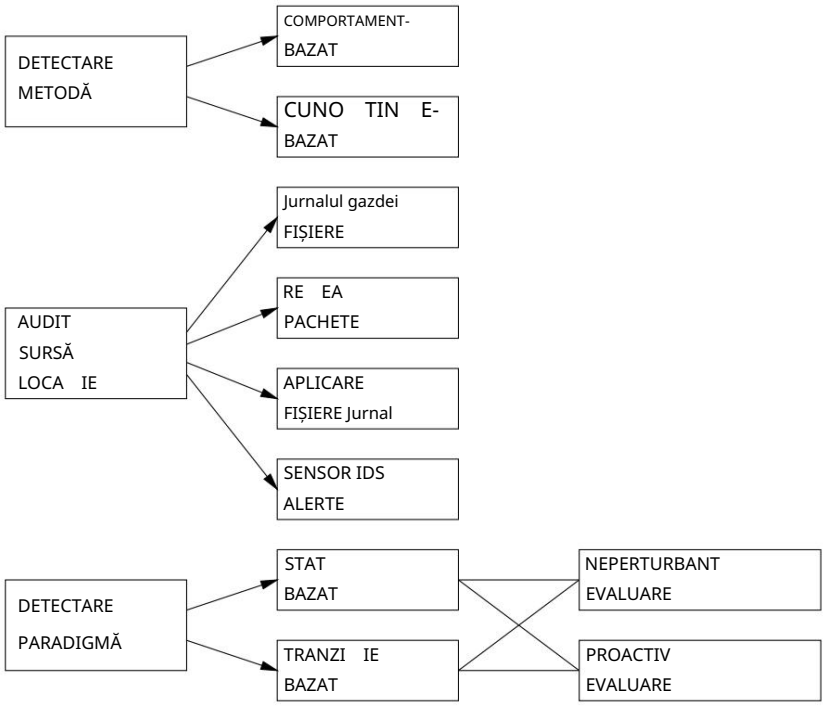


Figura 2: Caracteristicile sistemelor de detectare a intruziunilor.

Metoda de detectare descrie caracteristicile analizorului. Atunci când sistemul de detectare a intruziunilor folosește informații despre comportamentul normal al sistemului pe care îl monitorizează, îl calificăm ca fiind bazat pe comportament. Când sistemul de detectare a intruziunilor folosește informații despre atacuri, le calificăm ca fiind bazate pe cunoștințe.

Comportamentul la detectare descrie răspunsul sistemului de detectare a intruziunilor la atacuri. Când reacționează activ la atac, luând fie acțiuni corective (închiderea găurilor) fie pro-active (deconectarea posibililor atacatori, închiderea serviciilor), atunci se spune că sistemul de detectare a intruziunilor este activ. Dacă sistemul de detectare a intruziunilor generează doar alarme (cum ar fi paginarea), se spune că este pasiv.

Locația sursei de audit discriminează sistemele de detectare a intruziunilor pe baza tipului de informații de intrare pe care le analizează. Aceste informații de intrare pot fi trasee de audit (aka jurnalele de sistem) pe o gazdă, pachete de rețea, jurnalele de aplicații sau alerte de detectare a intruziunilor generate de alte sisteme de detectare a intruziunilor.

Paradigma de detectare descrie mecanismul de detectare utilizat de sistemul de detectare a intruziunilor. Sistemele de detectare a intruziunilor pot evalua stările (securizate sau nesigure) sau tranzițiile (de la sigur la nesigur).

În plus, această evaluare poate fi efectuată într-un mod neobstructiv sau prin stimularea activă a sistemului pentru a obține un răspuns.

4 Detectarea intruziunilor bazată pe cunoștințe versus pe bază de comportament

Există două tendințe complementare în detectarea intruziunilor: (1) să folosească cunoștințele acumulate despre atacuri și să caute dovezi ale exploatării acestor atacuri și (2) să construiască un model de referință al comportamentului obișnuit al sistemului informațional monitorizat și să caute abateri de la utilizarea observată.
Prima tendință este adesea denumită detectarea utilizării greșite [29, 34], dar și detectarea după aspect [53]. A doua tendință este denumită detectarea anomaliilor [29] sau detectarea prin comportament [53]. În această lucrare, folosim termenul de detectare a intruziunilor bazată pe cunoștințe pentru prima tendință, deoarece considerăm că descrie tehnica utilizată mai precis. A doua tendință este caracterizată de termenul de detectare a intruziunilor bazată pe comportament. Ambii termeni sunt definiți mai pe larg în continuare.

4.1 Detectarea intruziunilor bazată pe cunoștințe

Tehnicile de detectare a intruziunilor bazate pe cunoștințe aplică cunoștințele acumulate despre atacuri specifice și vulnerabilități ale sistemului. Sistemul de detectare a intruziunilor conține informații despre aceste vulnerabilități și caută încercări de a le exploata. Când este detectată o astfel de încercare, se declanșează o alarmă. Cu alte cuvinte, orice acțiune care nu este recunoscută în mod explicit ca un atac este considerată acceptabilă. Prin urmare, acuratețea sistemelor de detectare a intruziunilor bazate pe cunoștințe este considerată bună. Cu toate acestea, completitatea lor depinde de actualizarea regulată a cunoștințelor despre atacuri.

Avantajele abordărilor bazate pe cunoștințe sunt că au, teoretic, rate foarte scăzute de alarmă falsă și că analiza contextuală propusă de sistemul de detectare a intruziunilor este detaliată, facilitând ofițerului de securitate care utilizează acest sistem de detectare a intruziunilor să înțeleagă problema și să ia măsuri preventive sau corective.

Dezavantajele includ dificultatea de a culege informațiile necesare despre atacurile cunoscute și de a le ține la zi cu noile vulnerabilități și medii. Întreținerea bazei de cunoștințe a sistemului de detectare a intruziunilor necesită o analiză atentă a fiecărei vulnerabilități și, prin urmare, este o sarcină care necesită timp.
Abordările bazate pe cunoștințe trebuie, de asemenea, să se confrunte cu problema generalizării. Cunoștințele despre atacuri depind în mare măsură de sistemul de operare, versiune, platformă și aplicație. Sistemul de detectare a intruziunilor rezultat este, prin urmare, strâns legat de un mediu dat. De asemenea, detectarea atacurilor din interior care implică un abuz de privilegii este considerată mai dificilă, deoarece nicio vulnerabilitate nu este exploatată de către atacator.

4.1.1 Sisteme expert

Sistemele expert [37] sunt utilizate în principal de tehnicile de detectare a intruziunilor bazate pe cunoștințe. Sistemul expert conține un set de reguli care descriu atacurile. Evenimentele de audit sunt apoi traduse în fapte care poartă semnificația lor semantică în sistemul expert, iar motorul de inferență trage concluzii folosind aceste reguli și fapte. Această metodă mărește nivelul de abstractizare al datelor de audit prin atașarea unei semantice.

Limbile bazate pe reguli [21] sunt un instrument natural pentru modelarea cunoștințelor pe care experții le-au adunat despre atacuri. Această abordare permite o parcurgere sistematică a pistei de audit în căutarea dovezilor încercărilor de exploatare a vulnerabilităților cunoscute. De asemenea, sunt folosite pentru a verifica aplicarea corectă a politicii de securitate a unei organizații.

Raționamentul bazat pe model, care utilizează și sisteme expert, dar are proprietăți suplimentare, a fost introdus de Garvey și Lunt [19]. Cunoștințele despre comportamentul unui atacator sunt descrise de obiectivele atacatorului, de acțiunile pe care le întreprinde pentru a atinge aceste obiective și de utilizarea de către acesta a sistemului, care uneori dezvăluie un anumit nivel de paranoia. Instrumentul scanează apoi auditurile pentru dovezi ale acestor acțiuni și tranziții.

Această abordare de utilizare a limbajelor bazate pe reguli a arătat limitări în următoarele domenii:

Ingineria cunoștințelor (legată de problema completității): este dificil să extragi
cunoștințe despre atacuri. Este și mai dificil să transpuneți aceste cunoștințe în reguli de producție folosind audituri ca intrări. Uneori, informațiile necesare nu sunt disponibile în

auditurile. De asemenea, pot exista multe modalități de a exploata o anumită vulnerabilitate, ducând astfel la cât mai multe reguli.

Viteza de procesare (legată de problema de performanță):
Utilizarea unui shell de sistem expert necesită ca toate auditurile să fie importate în shell ca fapte și numai atunci poate avea loc raționamentul. Chiar dacă unele instrumente de sistem expert permit compilarea regulilor, performanța generală a instrumentului rămâne adesea scăzută.

Din cauza problemei vitezei de procesare, shell-urile de sistem expert sunt utilizate numai în prototipuri, ca comerciale produsele au ales abordări mai eficiente.

4.1.2 Analiza semnăturii

Analiza semnăturilor urmează exact aceeași abordare de achiziție de cunoștințe ca și sistemele expert, dar cunoștințele sunt exploatate într-un mod diferit. Descrierea semantică a atacurilor este transformată în informații care pot fi găsite în pista de audit într-un mod simplu. De exemplu, scenariile de atac pot fi traduse în secvențele de evenimente de audit pe care le generează sau în modele de date care pot fi căutate în pista de audit generată de sistem. Această metodă scade nivelul semantic al descrierilor de atac.

Această tehnică permite o implementare foarte eficientă și, prin urmare, este aplicată în produsele comerciale de detectare a intruziunilor [23, 28, 59]. Principalul dezavantaj al acestei tehnici - comun tuturor abordărilor bazate pe cunoștințe - este nevoia de actualizări frecvente pentru a ține pasul cu fluxul de noi vulnerabilități descoperite.
Această situație este agravată de cerința de a reprezenta toate fațetele posibile ale atacurilor prin semnături.
Acest lucru duce la un atac reprezentat de un număr de semnături, cel puțin una pentru fiecare sistem de operare la care a fost portat sistemul de detectare a intruziunilor.

4.2 Detectarea intruziunilor bazată pe comportament

Tehnicile de detectare a intruziunilor bazate pe comportament presupun că o intruziune poate fi detectată prin observarea unei abateri de la comportamentul normal sau așteptat al sistemului sau al utilizatorilor. Modelul comportamentului normal sau valid este extras din informațiile de referință colectate prin diverse mijloace. Sistemul de detectare a intruziunilor compară ulterior acest model cu activitatea curentă. Când se observă o abatere, se generează o alarmă.
Cu alte cuvinte, orice lucru care nu corespunde unui comportament învățat anterior este considerat intruziv.
Prin urmare, sistemul de detectare a intruziunilor ar putea fi complet, dar acuratețea sa este o problemă dificilă.

Avantajele abordărilor bazate pe comportament sunt că pot detecta încercările de a exploata vulnerabilități noi și neprevăzute. Ele pot chiar contribui la descoperirea (parțial) automată a acestor noi atacuri. Ele sunt mai puțin dependente de mecanismele specifice sistemului de operare. De asemenea, ajută la detectarea atacurilor de tip „abuz de privilegii” care nu implică de fapt exploatarea vreunei vulnerabilități de securitate.

Rata ridicată a alarmelor false este în general citată ca principalul dezavantaj al tehnicilor bazate pe comportament, deoarece nu întreaga sferă a comportamentului unui sistem informațional poate fi acoperită în timpul fazei de învățare.
De asemenea, comportamentul se poate schimba în timp, introducând necesitatea unei reinstruiri periodice on-line a profilului de comportament, rezultând fie indisponibilitatea sistemului de detectare a intruziunilor, fie alarme false suplimentare.
Sistemul informațional poate suferi atacuri în același timp în care sistemul de detectare a intruziunilor învață comportamentul. Ca urmare, profilul comportamental va conține un comportament intruziv, care nu este detectat ca anormal.

4.2.1 Statistici

Cel mai utilizat instrument pentru a construi sisteme de detectare a intruziunilor bazate pe comportament este statistica [25, 26, 31]. Comportamentul utilizatorului sau al sistemului este măsurat printr-un număr de variabile eșantionate în timp. Exemple de aceste variabile includ timpul de conectare și deconectare a fiecărei sesiuni, durata resursei și cantitatea de resurse procesor-memorie-disc consumată în timpul sesiunii. Perioada de eșantionare variază de la foarte scurtă (câteva minute) la lungă (o lună sau mai mult).

Modelul original păstrează mediile tuturor acestor variabile și detectează dacă pragurile sunt depășite pe baza abaterii standard a variabilei. De fapt, acest model este prea simplu pentru a reprezenta datele

cu fidelitate. Chiar și compararea variabilelor utilizatorilor individuali cu statisticile de grup agregate nu reușește să producă o îmbunătățire semnificativă. Prin urmare, a fost dezvoltat un model mai complex [30, 31] care compară profilurile activităților utilizatorilor pe termen lung și pe termen scurt. Profilurile sunt actualizate regulat pe măsură ce comportamentul utilizatorilor evoluează.
Acest model statistic este utilizat acum într-un număr de sisteme și prototipuri de detectare a intruziunilor.

4.2.2 Sisteme expert

De asemenea, sistemele expert au fost folosite pentru detectarea intruziunilor bazată pe comportament. Exemple de două abordări care au fost urmărite în acest domeniu sunt

- Wisdom & Sense [57], un sistem de detectare a intruziunilor care detectează anomalii statistice în comportamentul utilizatorilor. Instrumentul construiește mai întâi un set de reguli care descriu statistic comportamentul utilizatorilor pe baza înregistrărilor activităților lor într-o anumită perioadă de timp. Activitatea curentă este apoi comparată cu aceste reguli pentru a detecta comportamentul inconsecvent. Baza de reguli este reconstruită în mod regulat pentru a se adapta noilor modele de utilizare.

- ComputerWatch de la AT&T [13], un instrument livrat cu sistemul de operare de securitate multinivel UNIX/MLS de la AT&T. Acest instrument verifică acțiunile utilizatorilor conform unui set de reguli care descriu politica de utilizare adecvată și semnalează orice acțiune care nu se potrivește cu tiparele acceptabile.

Această abordare este utilă pentru profilurile de utilizare bazate pe politici, dar este mai puțin eficientă decât abordarea statistică pentru prelucrarea unor cantită i mari de informa ii de audit.

4.2.3 Rețele neuronale

Rețelele neuronale sunt tehnici algoritmice folosite pentru a învăța mai întâi relația dintre cele două seturi de informații, apoi pentru a „genera” pentru a obține noi perechi intrare-ieșire într-un mod rezonabil. Rețelele neuronale ar putea fi utilizate teoretic în sistemele de detectare a intruziunilor bazate pe cunoștințe pentru a identifica atacurile și a le căuta în fluxul de audit. Cu toate acestea, deoarece în prezent nu există o modalitate fiabilă de a înțelege ce a declanșat asocierea, rețeaua neuronală nu poate explica raționamentul care a condus la identificarea atacului.

În detectarea intruziunilor, rețelele neuronale au fost folosite în principal pentru a învăța comportamentul actorilor din sistem (de exemplu, utilizatori, demoni). A fost demonstrată o anumită echivalență între modelele de rețele neuronale și statistici [18, 48]. Avantajul utilizării rețelelor neuronale mai degrabă decât a statisticilor constă în a avea o modalitate simplă de a exprima relații neliniare între variabile și în învățarea/reformarea automată a rețelei neuronale. Experimentele au fost efectuate folosind o rețea neuronală pentru a prezice comportamentul utilizatorilor [8].
Aceste experimente au arătat că comportamentul utilizatorilor root UNIX este extrem de previzibil (datorită activității foarte regulate generate de acțiunile automate ale sistemului, demonii etc.), că comportamentul majorității utilizatorilor este, de asemenea, previzibil și că există doar o mică parte a utilizatorilor al căror comportament este imprevizibil.
Cu toate acestea, rețelele neuronale sunt încă o tehnică intensivă de calcul și nu sunt utilizate pe scară largă de comunitatea de detectare a intruziunilor.

4.2.4 Imunologie computerizată

Imunologia computerizată a fost descrisă de Forrest et al. [17]. Această tehnică încearcă să construiască un model al comportamentului normal al serviciilor de rețea UNIX, mai degrabă decât al comportamentului utilizatorilor. Acest model constă din secvențe scurte de apeluri de sistem efectuate de procese. Este posibil ca atacurile care exploatează defecte ale codului să treacă prin căi de execuție neutilizate de obicei. Instrumentul colectează mai întâi un set de audituri de referință, care reprezintă comportamentul adecvat al serviciului și extrage un tabel de referință care conține toate secvențele „bune” cunoscute de apeluri de sistem. Aceste modele sunt apoi folosite pentru monitorizarea live pentru a verifica dacă secvențele generate sunt listate în tabel; dacă nu, sistemul de detectare a intruziunilor generează o alarmă.

Această tehnică are o rată potențial foarte scăzută de alarmă falsă dacă tabelul de referință este suficient de exhaustiv.
În prezent sunt în curs de dezvoltare extensii pentru atingerea acestui obiectiv [9, 10]. Un dezavantaj, însă, este că această tehnică nu protejează împotriva erorilor de configurare într-un serviciu, adică atunci când atacurile folosesc acțiuni legitime ale serviciului pentru a obține acces neautorizat.

5 Detectarea intruziunilor bazată pe gazdă versus pe bază de rețea

Detectarea intruziunilor pe bază de gazdă a fost primul domeniu explorat în detectarea intruziunilor. Când au fost proiectate primele sisteme de detectare a intruziunilor, mediul țintă era un computer mainframe, iar toți utilizatorii erau locali în sistemul luat în considerare. Acest lucru a simplificat foarte mult sarcina de detectare a intruziunilor, deoarece interacțiunea din exterior era rară. Sistemul de detectare a intruziunilor a analizat informațiile de audit furnizate de mainframe, fie local [38], fie pe o mașină separată [50] și a raportat evenimente suspecte de securitate.

Pe măsură ce concentrarea calculului s-a mutat de la mediile mainframe la rețele distribuite de stații de lucru, au fost dezvoltate câteva prototipuri de sisteme de detectare a intruziunilor pentru a se adapta problemelor de rețea. Aici primul pas a fost să comunice sistemele de detectare a intruziunilor bazate pe gazdă [29]. Într-un mediu distribuit, utilizatorii trec de la o mașină la alta, eventual schimbând identitățile în timpul mișcărilor și lansează atacurile asupra mai multor sisteme. Prin urmare, sistemul local de detectare a intruziunilor de pe stația de lucru trebuie să facă schimb de informații cu colegii săi. Acest schimb de informații are loc la mai multe niveluri, fie prin schimbul unei piste de audit brute prin rețea, așa cum o face Stalker [23], fie prin emiterea de alarme bazate pe o analiză locală [51]. Ambele soluții implică costuri: transferul auditurilor poate avea un impact uriaș asupra lățimii de bandă a rețelei, în timp ce procesarea acestora la nivel local afectează performanța stației de lucru.

Odată cu utilizarea pe scară largă a Internetului, sistemele de detectare a intruziunilor s-au concentrat asupra atacurilor asupra rețelei în sine. Atacurile de rețea (falsificarea DNS, deturnarea TCP, scanarea portului, ping-ul morții etc.) nu pot fi detectate prin examinarea pistei de audit ale gazdei, sau cel puțin nu ușor. Prin urmare, au fost dezvoltate instrumente specifice care adulmecă pachetele de rețea în timp real, căutând astfel de atacuri de rețea. În plus, o serie de atacuri clasice împotriva serverelor pot fi detectate și prin analizarea sarcinii utile a pachetului și căutarea comenzilor suspecte. Mai mult, de multe ori aceste instrumente sunt atractive pentru administratorii de sistem deoarece un număr mic dintre ele pot fi instalate în puncte strategice din rețea pentru a acoperi majoritatea atacurilor actuale.

De asemenea, au fost dezvoltate abordări hibride care utilizează atât instrumente de detectare a intruziunilor bazate pe rețea, cât și pe gazdă într-un mediu cu mai multe gazdă. DIDS [51] folosește Haystack [50], care rulează pe fiecare gazdă pentru a detecta atacurile locale și NSM [24] pentru a monitoriza rețeaua. Ambele componente raportează Directorului DIDS, unde se face analiza finală.

Ca efect secundar, au apărut instrumente mai specializate de detectare a intruziunilor care monitorizează cele mai critice elemente ale prezenței unei organizații pe Internet. Aceste produse monitorizează firewall-urile (NetStalker [23]), serverele web (WebStalker [23]) sau routerele (NetRanger [7, 59]), căutând dovezi ale atacurilor în contextul extrem de specific al acestor elemente de rețea.

5.1 Surse de informații bazate pe gazdă

Sursele de audit ale gazdei sunt singura modalitate de a culege informații despre activitățile utilizatorilor unei anumite mașini. Pe de altă parte, ei sunt, de asemenea, vulnerabili la modificări în cazul unui atac reușit. Acest lucru creează o constrângere importantă în timp real asupra sistemelor de detectare a intruziunilor bazate pe gazdă, care trebuie să proceseze pista de audit și să genereze alarme înainte ca un atacator care preia mașina să poată submina fie pista de audit, fie sistemul însuși de detectare a intruziunilor.

5.1.1 Contabilitate

Contabilitatea este una dintre cele mai vechi surse de informații despre comportamentul sistemului. Oferă informații despre consumul de resurse partajate, cum ar fi timpul procesorului, memoria, utilizarea discului sau a rețelei și aplicațiile lansate de utilizatorii sistemului. Contabilitatea se găsește aproape peste tot, în echipamentele de rețea, în mainframe-uri precum și în stațiile de lucru UNIX. Această omniprezență i-a determinat pe unii designeri de prototipuri de detectare a intruziunilor să încerce să o folosească ca sursă de audit.

În mediul UNIX, contabilitatea este o sursă universală de informații. Formatul înregistrării contabile este același pe toate UNIX-urile, informațiile sunt comprimate pentru a câștiga spațiu pe disc, iar suprasarcina introdusă de procesul de înregistrare este foarte mică. Este bine integrat în sistemele de operare moderne și ușor de configurat și exploatat.

Cu toate acestea, informațiile contabile au și o serie de dezavantaje, care le fac nedemn de încredere din motive de securitate. În special, informațiile care identifică comanda lansată, precum și marcajele de timp sunt prea imprecise pentru a permite detectarea eficientă a atacurilor.

5.1.2 Syslog

Syslog este un serviciu de audit oferit aplicațiilor de către sistemul de operare (UNIX și altele). Acest serviciu primește un șir de text de la aplicație, îl prefixează cu un marcaj de timp și numele sistemului pe care rulează aplicația, apoi îl arhivează, fie local, fie de la distanță.

Se știe că Syslog are vulnerabilități de securitate, deoarece demonii Syslog de pe mai multe sisteme de operare UNIX au făcut obiectul documentelor CERT [5] care arată că depășirile de buffer din daemonul syslog pot fi exploatate pentru a executa cod arbitrar.

Syslog este foarte ușor de utilizat, iar acest lucru a determinat mulți dezvoltatori de aplicații să-l folosească ca pistă de audit. O serie de aplicații și servicii de rețea îl folosesc, cum ar fi login, sendmail, nfs, http, inclusiv instrumente legate de securitate, cum ar fi sudo, klaxon sau wrapper-uri TCP. Prin urmare, au fost dezvoltate câteva instrumente de detectare a intruziunilor care utilizează informațiile furnizate de demonul syslog, de exemplu Swatch [22]. Deși syslog este o sursă de audit ușoară care nu generează o cantitate mare de date de audit pe mașină, o rețea mare poate genera un număr mare de mesaje, dintre care foarte puține sunt relevante pentru securitate. Swatch [22] reduce sarcina administratorului de sistem prin corelarea mesajelor (rapoartele de la mai multe mașini că un server nfs este defect ar fi agregate într-una singură) și evidențiind cele legate de securitate.

5.1.3 Auditul de securitate C2

Auditul de securitate înregistrează toate evenimentele potențial semnificative pentru securitate din sistem. Întrucât guvernul SUA a cerut ca toate sistemele informatice pe care le achiziționează să fie certificate la nivelul C2 al TCSEC [56], toți furnizorii de sisteme de operare care concurează în acest domeniu au trebuit să includă o caracteristică de „responsabilitate”. Acest lucru se traduce în piste de audit de securitate, cum ar fi pachetele SUN BSM și Shield sau auditul AIX.

Toate aceste piste de audit de securitate au același principiu de bază: înregistrează încrucișarea instrucțiunilor executate de procesor în spațiul utilizator și instrucțiunilor executate în spațiul Trusted Computing Base (TCB) [56]. Acest model de securitate postulează că TCB este de încredere, că acțiunile din spațiul utilizatorului nu pot dăuna securității sistemului și că acțiunile legate de securitate care pot avea impact asupra sistemului au loc numai atunci când utilizatorii solicită servicii de la TCB.

În mediul UNIX, TCB este practic nucleul. Prin urmare, sistemul de audit înregistrează execuția apelurilor de sistem de către toate procesele lansate de utilizator. În comparație cu o urmărire completă a apelurilor de sistem, pista de audit oferă o abstractizare limitată: schimbările de context, alocarea memoriei, semaforele interne și citirile consecutive ale fișierelor nu apar în urma. Pe de altă parte, există întotdeauna o mapare simplă a evenimentelor de audit cu apelurile de sistem.

Înregistrarea de audit de securitate UNIX conține o cantitate mare de informații despre evenimente. Acesta include identificarea detaliată a utilizatorului și a grupului (de la identitatea de conectare la cea sub care este executat apelul de sistem), parametrii execuției apelului de sistem (numele fișierelor, inclusiv calea, argumentele liniei de comandă etc.), codul de retur de la execuție și codul de eroare.

Principalele avantaje ale auditului de securitate sunt

- o identificare puternică a utilizatorului, identitatea sa de autentificare, identitatea sa reală (actuală), identitatea sa efectivă (set-user-id bit), identitățile de grup reale și efective (set-group-id bit);
- o repartizare a evenimentelor de audit în clase pentru a facilita configurarea sistemului de audit;
- o parametrizare fină a informațiilor adunate în funcție de utilizator, clasă, eveniment de audit și eșecul sau succesul apelului de sistem și
- o oprire a mașinii în cazul în care sistemul de audit întâmpină o stare de eroare (de obicei, epuizarea spațiu pe disc).

Principalele dezavantaje ale auditului de securitate sunt

- o utilizare intensă a resurselor sistemului atunci când se solicită monitorizare detaliată. Performanța procesorului ar putea fi redusă cu până la 20%, iar cerințele pentru stocarea și arhivarea spațiului pe disc local sunt mari;
- un posibil atac de tip denial-of-service prin completarea sistemului de fișiere de audit;

- dificultatea înființării serviciului de audit din cauza numărului de parametri implicați. Configurațiile standard furnizate de furnizori minimizează performanța afectată prin înregistrarea numai a claselor de evenimente rare (acțiuni administrative, autentificare și deconectare). Cerințele de audit ale unui instrument de detectare a intruziunilor necesită informații mai detaliate, cum ar fi accesările la fișiere, procesele executate;

- dificultatea de a exploata informațiile obținute datorită dimensiunii și complexității acesteia. Acest lucru este agravat de eterogenitatea interfețelor sistemului de audit și a formatelor de înregistrări de audit în diferitele sisteme de operare și

- parametrizarea sistemului de audit care implică subiec i (utilizatori) i ac iuni (apeluri de sistem sau evenimente), i doar foarte rar obiecte (pe care se realizează ac iunea). Obiectele importante ar trebui monitorizate de un instrument de detectare a intruziunilor, iar acest lucru se face în primul rând prin scanarea întregului traseu.

Auditul de securitate C2 este sursa principală de informații de audit pentru majoritatea prototipurilor și instrumentelor de detectare a intruziunilor bazate pe gazdă, deoarece în prezent este singurul mecanism de încredere pentru a culege informații detaliate despre acțiunile întreprinse pe un sistem informatic. Au fost efectuate lucrări de mai multe grupuri [21, 39, 43, 55] pentru a defini ce informații ar trebui incluse în pista de audit de securitate, precum și un format comun pentru înregistrările urmăririi de audit, dar acesta este un efort de cercetare în curs de desfășurare.

5.2 Surse de informații bazate pe rețea

5.2.1 Informații SNMP

Basic Network Management Protocol (SNMP) Management Information Base (MIB) este un depozit de informații utilizate în scopuri de gestionare a rețelei. Conține informații de configurare (tabele de rutare, adrese, nume) și date de performanță/contabil (contoare pentru măsurarea traficului la diferite interfețe de rețea și la diferite straturi ale rețelei). Această secțiune descrie experimente efectuate în cadrul proiectului SECURENET [53] pentru a utiliza MIB comun SNMP V1 pentru Ethernet și TCP/IP. Alte proiecte vizează, de asemenea, utilizarea SNMPv2 și SNMPv3 pentru securitate și detectarea intruziunilor [32].

Proiectul SECURENET a explorat dacă contoarele menținute în acest MIB sunt utilizabile ca informații de intrare pentru un sistem de detectare a intruziunilor bazat pe comportament. Punctul de plecare a fost examinarea contoarelor la nivel de interfață deoarece acesta era singurul loc în care se putea diferenția între informațiile transmise prin fir și informațiile transmise în interiorul sistemului de operare prin interfața loop-back. Prototipul a colectat creșteri ale numărului de octeți și pachete transmise și primite la fiecare interfață la fiecare cinci minute. Rezultatul unei analize foarte simple a mediei/deviației standard a acestor date nu a fost satisfăcător, deoarece abaterea standard a fost mai mare decât media pentru aproape toate seturile colectate în timpul activității de zi.

Contoarele MIB de la nivelurile superioare ale rețelei nu conțin mult mai multe informații. Pe straturile IP, TCP și UDP, contoarele au prezentat un comportament similar, dar, din cauza numărului mai mare de contoare de la aceste straturi, nu am calculat toate corelațiile posibile. Contoarele ICMP arată mai multă consistență în ceea ce privește modelarea lor statistică, dar atacurile ICMP [4] nu au fost încercate pentru a valida această abordare.

Acest studiu arată că MIB-urile SNMP sunt un candidat potențial interesant ca sursă de audit pentru sistemele de detectare a intruziunilor. Dispariția SNMPv2 din cauza lipsei de consens cu privire la caracteristicile de securitate a scăzut cu siguranță interesul comunității de detectare a intruziunilor față de acesta. Cu toate acestea, odată cu implementarea SNMPv3, noi proiecte exploatează caracteristicile acestuia pentru instrumentele de detectare a intruziunilor [32].

5.2.2 Pachete de rețea

Pe măsură ce popularitatea sniffer-urilor de rețea pentru culegerea de informații a crescut în comunitatea atacatorilor, în prezent, aceștia sunt priviți și ca un mijloc eficient de strângere de informații despre evenimentele care au loc în arhitectura rețelei. Acest lucru este în concordanță cu tendința de trecere de la un model de calcul centralizat la unul distribuit, iar ritmul schimbării a crescut chiar odată cu diversificarea pe scară largă a Internetului. Cele mai multe accesări la computere sensibile au loc astăzi printr-o rețea și, prin urmare, capturarea pachetelor înainte de a intra pe server este probabil cea mai eficientă modalitate de a monitoriza acest server.

Este, de asemenea, în concordanță cu apariția atacurilor de refuzare a serviciului. Pe măsură ce companiile pun informații valoroase pe internet și chiar depind de el ca sursă de venit, perspectiva de a se închide pur și simplu

un site web creează o amenințare eficientă pentru organizația care îl conduce. Majoritatea acestor atacuri de refuzare a serviciului provin din rețea și trebuie detectate la nivel de rețea, deoarece un sistem de detectare a intruziunilor bazat pe gazdă nu are capacitatea de a obține acest tip de informații de audit.

Există o dualitate inerentă în sniffer-urile de rețea, care este evidentă și în lumea firewall-urilor cu diferențele sale între gateway-urile la nivel de aplicație și routerele de filtrare [3]. Dacă analiza este efectuată la un nivel scăzut prin efectuarea potrivirii modelelor, analizei semnăturii sau a unui alt fel de analiză a conținutului brut al pachetului TCP sau IP, atunci sistemul de detectare a intruziunilor își poate efectua analiza rapid. Aceasta este o abordare apatridă care nu ia în considerare informațiile despre sesiune, deoarece acestea din urmă ar putea acoperi mai multe pachete de rețea. Dacă sistemul de detectare a intruziunilor acționează ca un gateway de aplicație și analizează fiecare pachet în raport cu aplicația sau protocolul urmat, atunci analiza este mai amănunțită, dar și mult mai costisitoare. Aceasta este o analiză de stat. Rețineți că această analiză a nivelurilor superioare ale protocolului depinde și de mașina specială protejată, deoarece implementările protocoalelor nu sunt identice de la o stivă de rețea la alta.

Această abordare abordează mai multe probleme:

- Detectarea atacurilor specifice rețelei. Există o serie de atacuri de rețea, în special atacuri de refuz de serviciu, care nu pot fi detectate în timp util prin căutarea informațiilor de audit pe gazdă, ci doar prin analizarea traficului de rețea.

- Impactul auditului asupra performanței gazdei. Informațiile sunt colectate în întregime pe o mașină separată, fără cunoștințe despre restul rețelei. Prin urmare, instalarea unor astfel de instrumente este facilitată deoarece nu afectează întregul mediu în ceea ce privește configurația și performanța.

- Formatele eterogene ale pistelor de audit. Actuala standardizare de facto față de TCP/IP facilitează achiziția, formatarea și analiza multiplatformă a informațiilor de audit.

- Anumite instrumente analizează sarcina utilă a pachetului, ceea ce permite ca atacurile împotriva gazdelor să fie detectate prin analiza semnăturii. Cu toate acestea, o analiză eficientă necesită cunoașterea tipului de mașină sau aplicație pentru care este destinat pachetul.

Dar are și o serie de dezavantaje:

- Este mai dificil să identifici vinovatul atunci când a fost descoperită o intruziune. Nu există o legătură sigură între informațiile conținute în pachete și identitatea utilizatorului care a trimis efectiv comenzile pe gazdă.

- În cazul rețelelor comutate (Ethernet comutat, Token-Ring comutat, ATM), selectarea unei locații adecvate pentru sniffer nu este simplă. Unele instrumente sunt situate pe comutatoare, altele la porțile de acces între sistemul protejat și lumea exterioară. Primul oferă informații de audit mai bune, dar implică și un cost mai mare. Rețineți, totuși, că rețelele comutate sunt, de asemenea, mult mai puțin vulnerabile la atacurile sniffer [6, 44] și sunt de fapt o soluție recomandată pentru a îmbunătăți securitatea unei rețele.

- Criptarea împiedică analiza încărcăturii utile a pachetelor și, prin urmare, ascunde o cantitate considerabilă de informații importante din aceste instrumente. De asemenea, chiar și fără criptare, este posibil să se ofusca conținutul pachetului pentru a evita detectarea [44] dacă semnăturile nu sunt suficient de cuprinzătoare.

- Scanarea sistematică, de exemplu la firewall, este dificilă deoarece poate crea blocaje. Acest lucru se va înrăutăți doar pe măsură ce lățimea de bandă pentru accesul la Internet crește pe site-urile sensibile (de exemplu, bănci, site-uri web de comerț electronic).

- În cele din urmă, aceste instrumente sunt în mod inerent vulnerabile la atacurile de refuzare a serviciului dacă se bazează pe un sistem de operare comercial pentru a obține informații de rețea. Așa cum stivele de rețea ale acestor sisteme de operare comerciale sunt vulnerabile la atacuri, la fel este și sistemul de detectare a intruziunilor.

Pachetele de rețea sunt în prezent sursa de informații utilizate de mai multe produse comerciale recente [7, 28, 59] și mai multe proiecte din comunitatea de cercetare urmăresc, de asemenea, această cale [41, 45, 46, 54]. O evaluare recentă a acestor produse de către Ptacek și Newsham [44] arată că abordarea sniffer, sau cel puțin implementările actuale, au defecte care fac posibil ca un atacator calificat să evite detectarea. În special, ele arată că fragmentarea IP nu este gestionată bine și că utilizarea metacaracterilor și a secvențelor de control în protocoale precum http face posibilă evitarea detectării prin semnătură. Tot în acest domeniu se efectuează cercetări. După IDES și NIDES, SRI dezvoltă acum un prototip numit Emerald [42] pentru a se ocupa de analiza traficului de rețea. Alte sniffer de rețea, cum ar fi Bro [41] sau Network Flight Recorder [45] au fost dezvoltate ca instrumente de achiziție de date în rețea și, prin urmare, nu acceptă detectarea intruziunilor în sine.

5.3 Fișiere jurnal de aplicație

Pe măsură ce tendința către serverele de aplicații devine mai pronunțată și noțiunea de sistem de operare se estompează, fișierele jurnal de aplicații capătă o importanță mai mare ca sursă de date pentru detectarea intruziunilor.

În comparație cu auditurile de sistem sau cu pachetele de rețea, utilizarea fișierelor jurnal de aplicații are trei avantaje:

Precizie. Datele de audit C2 sau pachetele de rețea necesită procesare înainte ca sistemul de detectare a intruziunilor să poată înțelege ce informații au fost de fapt primite de aplicație. Această prelucrare se bazează pe interpretări ale specificațiilor protocolului sau ale specificațiilor API și este probabil ca interpretarea dezvoltatorului aplicației să difere de cea a dezvoltatorului sistemului de detectare a intruziunilor. Obținând informațiile direct din jurnal, acuratețea informațiilor este aproape garantată.

Completitudine. Datele de audit C2 sau pachetele de rețea necesită reasamblarea mai multor apeluri de audit sau a mai multor pachete de rețea, potențial pe mai multe gazde, pentru a reconstrui sesiunea la nivel de aplicație, ceea ce poate fi foarte dificil de realizat. Mai mult decât atât, nici măcar o simplă reasamblare, cum ar fi potrivirea cererii http de intrare și a răspunsului de ieșire pentru a determina succesul unei cereri, nu este realizată de instrumentele curente. Jurnalul aplicației, pe de altă parte, conține toate informațiile relevante, chiar dacă aplicația este distribuită pe un cluster de mașini (de exemplu, server web sau server de baze de date). În plus, aplicația poate furniza date interne care nu apar în traseele de audit sau în pachetele de rețea.

Performan ă. Lăsând aplicația să selecteze informațiile relevante pentru scopuri de securitate, costul general indus de mecanismul de colectare este mult redus în comparație cu pistele de audit de securitate.

Există două dezavantaje în utilizarea fișierelor jurnal de aplicații pentru detectarea intruziunilor:

Stare de cursă. Atacurile sunt detectate numai atunci când este scris jurnalul aplicației. Dacă atacul poate împiedica scrierea jurnalului de aplicație (acest lucru poate fi cazul în multe atacuri de tip denial-of-service), atunci informațiile necesare sistemului de detectare a intruziunilor nu sunt acolo.

Atacurile la nivel scăzut. Există o serie de atacuri (din nou, în special atacuri de refuz de serviciu) care vizează nivelurile inferioare ale software-ului de sistem, cum ar fi driverele de rețea. Deoarece aceste atacuri nu exercită codul aplicației, este posibil să nu apară în jurnalele aplicației sau doar consecința atacului (cum ar fi repornirea) este vizibilă.

Un exemplu de astfel de instrument este WebWatcher [1], care monitorizează jurnalele serverului web în timp real și oferă informații mult mai detaliate despre atacurile pe servere web decât fac omologii săi din rețea. O abordare similară ar putea fi concepută pentru serverele de baze de date.

6 Paradigma de detectare

6.1 Sisteme de detectare a intruziunilor bazate pe stare versus tranziție

Există în esență două paradigme în motoarele de detectare a intruziunilor. Prima clasă de motoare de detectare a intruziunilor funcționează pe stări, a doua pe tranziții între stări. Figura 3 explică paradigma folosind

termeni definiți în fiabilitatea [2]. normal reprezintă starea dorită a sistemului. error1 și error2 reprezintă doi pași dintr-un lanț care va duce în cele din urmă la o stare de eșec. Scopul sistemului de detectare a intruziunilor este de a detecta că sistemul a părăsit starea normală înainte de a ajunge în starea de defecțiune. În contextul detectării intruziunilor, eroarea1 ar putea însemna că o versiune vulnerabilă a unei aplicații este instalată pe sistem. Dacă această aplicație vulnerabilă este folosită de atacator pentru a recupera fișierul passwd, atunci sistemul ar fi în starea error2. Starea finală de eșec ar putea reprezenta faptul că un atacator extern se conectează cu privilegii administrative.

Pentru a-și atinge scopul, instrumentele de detectare a intruziunilor pot face mai multe lucruri:

- Recunoașteți starea normală. Acest lucru este util doar moderat, deoarece nu oferă informații despre locul în care se află sistemul în lanțul către starea de defecțiune. De asemenea, este extrem de dificil să caracterizați normalitatea, așa cum sa discutat mai devreme în contextul detectării intruziunilor bazate pe comportament.
- Recunoașteți unele stări de eroare pe drum. De obicei, este posibil să se caracterizeze într-un fel stările de eroare care permite detectarea.
- Recunoașteți o anumită tranziție care duce la o stare de eroare.

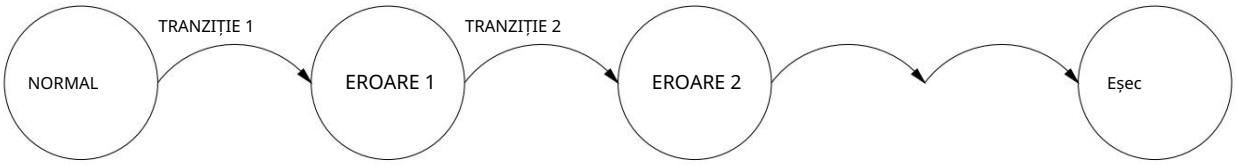


Figura 3: Stare versus tranziție.

Exemple de sisteme de detectare a intruziunilor bazate pe stat includ instrumente de evaluare a securității, cum ar fi COPS [14, 16] și Tiger [47] pentru mediile gazdă și Nessus [12], Satan [15] și Ballista [49] pentru instrumente bazate pe rețea. Aceste instrumente identifică stările de eroare când este prezentă o aplicație vulnerabilă sau o eroare de configurare.
Ei interogează sistemul pentru versiunile sau configurațiile aplicației și semnalează o stare de eroare atunci când versiunea sau configurația se potrivește cu informațiile din baza lor de vulnerabilități. Tripwire [33] păstrează semnăturile fișierelor importante și caută modificări. Astfel de modificări ar putea indica faptul că sistemul se află acum într-o stare de eroare (de exemplu, deoarece atacatorul a schimbat unul dintre fișierele originale cu un cal troian pentru o penetrare ușoară). Totuși, un alt sistem este Wisdom & Sense [57], care păstrează regulile statistice de comportament adecvat și indică când aceste reguli nu sunt îndeplinite (de exemplu, deoarece persoana din spatele terminalului se preface drept utilizator autorizat, dar nu se comportă exact așa cum se aștepta). Niciunul dintre aceste instrumente nu va detecta tranziția atunci când sistemul trece de la o stare la alta.

Exemple de sisteme de detectare a intruziunilor bazate pe tranziție includ NetRanger [7] sau RealSecure [28] pentru instrumente bazate pe rețea și USTAT [27] pentru instrumente bazate pe gazdă. Aceste instrumente urmăresc evenimente specifice despre care se știe că declanșează tranziția de la o stare la alta (de exemplu, atacuri, acțiuni rău intenționate, pachete rău intenționate).
USTAT are capacitatea de a combina mai multe tranziții, în timp ce RealSecure și NetRanger caută tranziții individuale.

6.2 Analiză neperturbătoare versus proactivă a stării sau a tranziției

Analiza stării sau a tranziției poate fi efectuată în două moduri, fie printr-o observare neperturbătoare a sistemului, fie printr-o încercare proactivă de a evalua starea sau tranziția care va modifica ulterior starea sistemului.

6.2.1 Analiză neperturbătoare

Într-o observație neperturbătoare, partea de evaluare a vulnerabilităților solicită versiuni de aplicație sau bannere și le compară cu un tabel de vulnerabilități cunoscute. Dacă versiunea aplicației este în tabel,

atunci sistemul este etichetat ca fiind în starea vulnerabilă, altfel va fi etichetat ca fiind în starea securizată. Acest tip de sondă încearcă să minimizeze impactul asupra sistemului în timp ce investighează în mod fiabil starea sau tranziția acestuia.

COPS sau SATAN sunt exemple de instrumente neperturbatoare, de analiză a stării. Cerând informații despre versiune de la aplicații și analizând fișierul de configurare, aceștia determină dacă sistemul este într-o stare securizată.

Exemple de instrumente de analiză a tranziției neperturbătoare includ instrumente de analiză a traficului de jurnal sau de rețea, cum ar fi RealSecure, NetRanger sau WebWatcher [1]. Aceste instrumente dobândesc informații în mod transparent, fie prin captarea pachetelor de rețea, fie prin primirea de intrări de jurnal, dar nu au un impact semnificativ asupra mediului în care rulează.

6.2.2 Analiză proactivă

O altă clasă de instrumente realizează o analiză proactivă declanșând în mod explicit evenimente în mediu pentru a determina stări sau pentru a crea tranziții.

Nessus sau Ballista sunt exemple de instrumente proactive, de analiză de stat. Ei exploatează în mod activ vulnerabilitățile pentru a determina starea sistemului. Aceste încercări sunt aproape imposibil de distins de cele nedorite și pot declanșa o tranziție de la o stare de eroare la următoarea din lanț.

Detectorul Sniffer [20] și AntiSniff [35] urmăresc detectarea snifferelor pasive care ar fi putut fi instalate într-o rețea pentru a captura date sensibile. Dacă este instalat un sniffer, sistemul ar fi într-o stare de eroare.
AntiSniff declanșează în mod proactiv efecte secundare în sniffer, care ar detecta starea de eroare dacă aceste efecte secundare sunt observate. Detectorul Sniffer introduce în mod proactiv momeli în sistem și caută dovezi ale utilizării acestor momeli. Dacă se găsesc astfel de dovezi, arată trecerea de la starea de eroare cu sniffer-ul instalat la următoarea stare de eroare în care proprietarul sniffer-ului folosește informațiile colectate.

7 Proprietăți suplimentare

7.1 Monitorizare continuă versus analiză periodică

Detectarea intruziunilor continuă versus periodică se aplică modului în care instrumentul își realizează analiza. Un instrument dinamic de detectare a intruziunilor efectuează o analiză continuă, în timp real, prin achiziționarea de informații despre acțiunile întreprinse asupra mediului imediat după ce acestea au loc. Un instrument static de detectare a intruziunilor realizează periodic un instantaneu al mediului și analizează acest instantaneu, căutând software vulnerabil, erori de configurare și așa mai departe.

Instrumentele statice evaluează nivelul de securitate al configurației curente a mediului. Exemplele includ COPS [14, 16] și Tiger [47] pentru mediile gazdă și Satan [15] și Ballista1 [49] pentru rețele. În aceeași categorie se află detectorii de viruși, care scanează discurile în căutarea modelelor de identificare a virușilor cunoscuți. Aceste verificări includ verificarea versiunii aplicațiilor instalate pentru a se asigura că au fost aplicate cele mai recente corecții de securitate, verificarea parolelor slabe, verificarea conținutului fișierelor speciale din directoarele de acasă ale utilizatorilor și verificarea configurației serviciilor de rețea deschise. Această analiză oferă o imagine instantanee a stării sistemului, dar este valabilă doar în acel moment precis.

Aceste instrumente sunt bine cunoscute și utilizate pe scară largă de către administratorii de sistem, dar nu sunt suficiente pentru a asigura o securitate ridicată. În primul rând, corecțiile de securitate nu sunt neapărat disponibile pe sistemele vechi, care nu pot fi actualizate fără a-și pierde cerințele operaționale. Mai mult decât atât, rularea acestor instrumente de evaluare a securității este adesea un proces lung, în special într-un mediu de rețea în care fiecare sistem trebuie verificat individual. Prin urmare, expunerea la securitate între două rulări consecutive poate fi semnificativă, aproximativ o zi întreagă și s-a demonstrat că exploatarea activă a vulnerabilităților pe Internet poate dura mai puțin de o zi.

1Acum CyberCop Scanner [40] de la achiziționarea Secure Networks de către Network Associates Inc.

Aceste instrumente, precum și altele dezvoltate special în acest scop, cum ar fi Tripwire [33] și ATP [58], pot fi utilizate pentru a detecta urmele unei intruziuni. Astfel de urme pot fi înlocuirea unei aplicații date cu una mai veche, vulnerabilă, care ar fi semnalată de COPS [14] și Tiger [47] administratorului de sistem ca o potențială intruziune. Tripwire [33] extinde acest principiu prin calcularea semnăturii unui set mare de fișiere de sistem și comparându-l cu o bază de date de semnături de referință păstrate într-un loc sigur, făcând astfel procesul de detectare a schimbărilor sistematic. O alarmă de către un sistem asemănător Tripwire semnalează o intruziune într-un mod bazat pe comportament, adică, că un anumit fișier din sistem nu mai este ceea ce era înainte.

Instrumentele dinamice de detectare a intruziunilor monitorizează acțiunile care au loc pe sistem. Monitorizarea are loc fie în timp real, fie în lot, adică revizuirea fișierelor de audit sau a pachetelor de rețea acumulate într-o anumită perioadă de timp. Monitorizarea dinamică presupune o analiză în timp real și permite o evaluare constantă a securității sistemului. Este, însă, un proces costisitor, atât pentru transportul auditurilor, cât și pentru prelucrarea acestora.

7.2 Protecția sistemului de detectare a intruziunilor

Atunci când este instalat un sistem de detectare a intruziunilor, acesta devine ținta principală naturală a atacurilor ostile, cu scopul de a dezactiva caracteristica de detectare și de a permite unui atacator să opereze fără a fi detectat.
Dezactivarea sistemului de detectare a intruziunilor se poate întâmpla în următoarele moduri:

Atacurile de refuzare a serviciului. Atacurile de refuzare a serviciului sunt o modalitate puternică și relativ simplă de a dezactiva temporar sistemul de detectare a intruziunilor. Atacul poate avea loc împotriva detectorului, forțându-l să prelucreze mai multe informații decât poate gestiona (de exemplu, prin saturarea unei legături de rețea). Acest lucru are de obicei efectul de a întârzia detectarea atacului sau, în cel mai rău caz, de a încurca suficient detectorul, astfel încât să rateze un element critic al atacului. O a doua posibilitate este saturarea capacității de reacție a operatorului care manipulează sistemul de detectare a intruziunilor. Atunci când operatorului i se prezintă prea multe alarme, poate să rateze cu ușurință cea importantă care indică pătrunderea, chiar dacă este prezentă pe ecran.

Sustragerea de la detectie. Au fost dezvoltate mai multe tehnici pentru a evita detectarea unui atac de către sistemele de detectare a intruziunilor. Instrumentele bazate pe rețea, cele mai populare instrumente astăzi, suferă în special de aceste atacuri care implică pachete de rețea realizate manual:

1. Atacul prin fragmentare IP. Sistemele de detectare a intruziunilor au dificultăți în reasamblarea pachetelor IP. Prin urmare, împărțirea artificială a unui atac în mai multe pachete creează o nepotrivire între datele din pachet și semnătură, ascunzând astfel atacul.
2. Atacă prin TTL (Time To Live). Prin modificarea TTL-ului pachetelor IP, este posibil ca sistemul de detectare a intruziunilor să vadă pachete care nu vor ajunge la ținta atacului. Prin inserarea de date false în fluxul de comunicare, un atacator poate intercala atacul cu informații false, ascunzând astfel atacul de sistemul de detectare a intruziunilor, în timp ce ținta reconstruiește corect aceste date de atac și reacționează la ele.

O descriere bună a diferitelor tehnici de atac și a modului în care sistemele de detectare a intruziunilor reacționează la acestea este oferită de Ptacek și Newsham [44]. Sistemele de detectare a intruziunilor încep să se protejeze de aceste atacuri, dar vânzătorii eliberează puține informații cu privire la eficacitatea acestor măsuri de protecție.

În plus, este adesea dificil de afirmat configurația unui sistem de detectare a intruziunilor, ca în majoritatea cazuri nu există o modalitate ușoară de a verifica configurația și detectarea corectă a atacurilor.

8 Concluzii și direcții viitoare

Detectarea intruziunilor atrage în prezent un interes considerabil atât din partea comunității de cercetare, cât și din partea companiilor comerciale. Prototipurile de cercetare continuă să apară, iar produse comerciale bazate pe cercetări timpurii sunt acum disponibile. În această lucrare, am oferit o imagine de ansamblu asupra stadiului actual al tehnicii de detectare a intruziunilor, bazată pe o taxonomie propusă ilustrată cu exemple de proiecte trecute și actuale. Taxonomia clar

evidențiază proprietățile acestor sisteme de detectare a intruziunilor, acoperind în mod adecvat atât evoluțiile trecute, cât și actualele.

Sursele de informații pentru aceste instrumente sunt fie o pistă de audit C2, syslog, fie pachete de rețea. În timp ce sursele de sistem au fost utilizate pe scară largă în etapele incipiente ale cercetării, concentrarea actuală a prototipurilor de cercetare, precum și a produselor este pe protejarea infrastructurii mai degrabă decât a stației utilizatorului final, iar această paradigmă a condus la utilizarea sniffer-urilor de rețea care analizează pachetele. După cum se arată, un număr destul de mare de probleme de cercetare referitoare la eficiența surselor de audit ale rețelei și gazdă, formatarea și existența unui format comun de urmărire de audit și chiar conținutul pistei de audit în sine, încă așteaptă un răspuns.

Există, de asemenea, o serie de probleme nerezolvate cu privire la analiza pistei de audit. Analiza semnăturilor este în mod clar în domeniul comercial acum, dar s-a dovedit a fi insuficientă pentru detectarea tuturor atacurilor.
Prin urmare, se lucrează încă pentru a experimenta noi abordări atât pentru detectarea intruziunilor bazată pe cunoștințe, cât și pe cea bazată pe comportament. Detectarea atacurilor de abuz de privilegii (în primul rând atacuri din interior) face, de asemenea, obiectul unor lucrări în desfășurare.

Referințe

[1] Magnus Almgren, Hervée Debar și Marc Dacier. Un instrument ușor pentru detectarea atacurilor pe serverele web. În Gene Tsudik și Avi Rubin, editori, Proceedings of NDSS 2000 (Network and Distributed System Security Symposium), paginile 157–170, San Diego, CA, februarie 2000. The Internet Society.

[2] T. Anderson, A. Avizienis, WC Carter, A. Costes, F. Cristian, Y. Koga, H. Kopetz, JH Lala, JC Laprie, JF Meyer, B. Randell, AS Robinson, L. Simonici și U. Voges. Fiabilitate: concepte de bază și terminologie. Calcul de încredere și toleranța la erori. Springer Verlag, 1992.

[3] Steven M. Bellovin și William R. Cheswick. Firewall-uri de rețea. IEEE Communications MAGAZINE, 32(9):50–57, septembrie 1994.

[4] Centrul de coordonare CERT. Atacul de refuzare a serviciului prin ping. Disponibil prin ftp anonim de la ftp.cert.org, decembrie 1986.

[5] Centrul de coordonare CERT. Vulnerabilitatea Syslog - o soluție pentru sendmail. Disponibil de către anonim ftp de pe ftp.cert.org, octombrie 1995.

[6] William R. Cheswick și Steven M. Bellovin. Firewall-uri și securitate pe internet – respingerea șmecherilor Hacker. Seria de calcul profesional. Addison-Wesley, 1994. ISBN 0-201-63357-4.

[7] Cisco Systems Inc. NetRanger – Sistem de detectare a intruziunilor în rețea, la scară întreprindere, în timp real. Internet http://www.cisco.com/, 1998.

[8] Hervée Debar, Monique Becker și Didier Siboni. O componentă de rețea neuronală pentru un sistem de detectare a intruziunilor. În Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, paginile 240–250, Oakland, CA, mai 1992.

[9] Hervée Debar, Marc Dacier, Medhi Nassehi și Andreas Wespi. Modele fixe vs. cu lungime variabilă pentru detectarea comportamentului suspect al procesului. În Jean-Jacques Quisquater, Yves Deswarte, Catherine Meadows și Dieter Gollmann, editori, Computer Security - ESORICS 98, 5th European Symposium on Research in Computer Security, volumul 1485 din LNCS, paginile 1–15, Louvain-la-Neuve, Belgia, septembrie 1998. Editura Springer.

[10] Hervée Debar, Marc Dacier și Andreas Wespi. Generarea de informații de audit de referință pentru sistemele de detectare a intruziunilor. În Reinhard Posch și Gy¨orgy Papp, editori, Information Systems Security, Proceedings of the 14th International Information Security Conference IFIP SEC'98, paginile 405–417, Viena, Austria și Budapesta, Ungaria, 31 august – 4 septembrie 1998.

[11] Dorothy Denning. Un model de detectare a intruziunilor. Tranzacții IEEE privind inginerie software, 13(2):222–232, 1987.

[12] Renaud Deraison. Proiectul nessus. http://www.nessus.org/documentation.html, 1999.

[13] Cheri Dowell și Paul Ramstedt. Instrumentul de reducere a datelor ComputerWatch. În Proceedings of the 13th National Computer Security Conference, paginile 99–108, Washington, DC, octombrie 1990.

[14] Dan Farmer. Prezentare generală a polițiștilor. Disponibil de la http://www.trouble.org/cops/overview.html, mai 1993.

[15] Dan Farmer și Wietse Venema. Îmbunătățirea securității site-ului tău prin spargere în el. disponibil la http://www.trouble.org/security/admin-guide-to-cracking.html, 1993. Carte albă pentru Internet.

[16] Daniel Farmer și Eugene Spafford. Sistemul de verificare a securității polițiștilor. În Proceedings of Summer Conferința USENIX, paginile 165–170, Anaheim, CA, iunie 1990.

[17] Stephanie Forrest, Steven A. Hofmeyr și Anil Somayaji. Imunologie computerizată. Comunicări ale ACM, 40(10):88–96, octombrie 1997.

[18] Patrick Gallinari, Sylvie Thiria și Francoise Fogelman-Soulie. Perceptroni multistrat și analiza datelor. În Proceedings of the IEEE Annual International Conference on Neural Networks (ICNN88), volumul I, paginile 391–399, San Diego, CA, iulie 1988.

[19] Thomas Garvey și Teresa Lunt. Detectarea intruziunilor pe bază de model. În Proceedings of the 14th National Computer Security Conference, paginile 372–385, octombrie 1991.

[20] Stephane Grundschober. Proiectarea și implementarea unui detector sniffer. În Proceedings of RAID 98, Workshop on Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgia, septembrie 1998.

[21] Naji Habra, Baudouin Le Charlier, Aziz Mounji și Isabelle Mathieu. Asax: Arhitectură software și limbaj bazat pe reguli pentru analiza universală a pistei de audit. În Y. Deswarte, G. Eizenberg și J.-J. Quisquater, editori, Proceedings of the Second European Symposium on Research in Computer Security (ESORICS), volumul 648 din Lecture Notes in Computer Science, Toulouse, Franța, noiembrie 1992. Springer-Verlag, Berlin Germania.

[22] Stephen E. Hansen și E. Todd Atkins. Monitorizare automată a sistemului și notificare cu swatch. În Proceedings of the seventh Systems Administration Conference (LISA '93), Monterey, CA, noiembrie 1993.

[23] Haystack Labs, Inc. Stalker. http://www.haystack.com/stalk.htm, 1997.

[24] L. Todd Heberlein, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood și David Wolber. Un monitor de securitate a rețelei. În Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, paginile 296–304, Oakland, CA, mai 1990. IEEE Computer Society Press, Los Alamitos, CA.

[25] Paul Helman și Gunar Liepins. Bazele statistice ale analizei pistelor de audit pentru detectarea utilizării greșite a computerului. IEEE Transactions on Software Engineering, 19(9):886–901, septembrie 1993.

[26] Paul Helman, Gunar Liepins și Wynette Richards. Bazele detectării intruziunilor. În Proceedings of the Fifth Computer Security Foundations Workshop, paginile 114–120, Franconic, NH, iunie 1992.

[27] Koral Ilgun. Ustat: Un sistem de detectare a intruziunilor în timp real pentru Unix. În Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, paginile 16–28, Oakland, CA, mai 1993.

[28] Internet Security Systems, Inc. RealSecure. Internet http://www.iss.net/prod/rsds.html, 1997.

[29] R. Jagannathan, Teresa Lunt, Debra Anderson, Chris Dodd, Fred Gilham, Caveh Jalali, Hal Javitz, Peter Neumann, Ann Tamaru și Alfonso Valdes. Document de proiectare a sistemului: Sistemul expert de detectare a intruziunilor de ultimă generație (NIDES). Raport tehnic A007/A008/A009/A011/A012/A014, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025, martie 1993.

[30] Harold Javitz și Alfonso Valdes. Detectorul de anomalii statistice SRI IDES. În Proceedings of the Simpozionul IEEE privind cercetarea în securitate și confidențialitate, paginile 316–326, mai 1991.

[31] Harold S. Javitz, Alfonso Valdez, Teresa F. Lunt, Ann Tamaru, Mabry Tyson și John Lowrance. Sistemul expert de detectare a intruziunilor de ultimă generație (NIDES) - 1. rațiunea algoritmilor statistici - 2. rațiunea soluției propuse. Raport tehnic A016–Rationales, SRI International, 333 Ravenswood Avenue, Menlo Park, CA, martie 1993.

[32] Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun Felix Wu și W. Rance Cleaveland. Proiectarea arhitecturii unui sistem scalabil de detectare a intruziunilor pentru infrastructura de rețea emergentă. Raport tehnic CDRL A005, MCNC Information Technologies Division, Research Triangle Park, NC 27709, aprilie 1997.

[33] Gene H. Kim și Eugene H. Spafford. Proiectarea și implementarea tripwire: un verificator de integritate a sistemului de fișiere. În Jacques Stern, editor, a 2-a Conferință ACM privind securitatea computerelor și comunicațiilor, paginile 18–29, COAST, Purdue, noiembrie 1994. ACM Press.

[34] Sandeep Kumar și Eugene Spafford. Un model de potrivire a modelelor pentru detectarea intruziunilor de utilizare greșită. În Proceedings of the 17th National Computer Security Conference, paginile 11–21, octombrie 1994.

[35] Inc. L0pht Heavy Industries. Ce este adulmecarea pachetelor. http://www.l0pht.com/antisniff/overview.html, 1999.

[36] Carl E. Landwehr, Alan R. Bull, John P. McDermott și William S. Choi. O taxonomie a defectelor de securitate a programelor de calculator. ACM Computing Surveys, 26(3):211–254, septembrie 1994.

[37] Teresa Lunt și R. Jagannathan. Un prototip de sistem expert de detectare a intruziunilor în timp real. În Proceed-ings of the 1988 Symposium on Security and Privacy, paginile 59–66, Oakland, CA, aprilie 1988.

[38] Teresa F. Lunt, R. Jagannathan, Rosanna Lee, Sherry Listgarten, David L. Edwards, Peter G. Neumann, Harold S. Javitz și Alfonso Valdes. IDES: Prototipul îmbunătățit – un sistem expert de detectare a intruziunilor în timp real. Raport tehnic SRI-CSL-88-12, SRI International, 333 Ravenswood Avenue, Menlo Park, CA, octombrie 1988.

[39] Abdelaziz Mounji. Limbi și instrumente pentru detectarea intruziunilor distribuite pe bază de reguli. Doctor în științe, Facultăți Universitaires Notre-Dame de la Paix, Namur (Belgia), septembrie 1997.

[40] Network Associates Inc. Scanner Cybercop. Disponibil pe site-ul web al companiei la http://www.nai.com/products/security/ballista/default.asp, 1998.

[41] Vern Paxson. Bro: Un sistem pentru detectarea intrușilor din rețea în timp real. În Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, ianuarie 1998.

[42] Phillip A. Porras și Alfonso Valdes. Analiza live a traficului gateway-urilor tcp/ip. În Proceedings of the 1998 ISOC Symposium on Network and Distributed System Security (NDSS'98), San Diego, CA, martie 1998. Internet Society.

[43] Katherine E. Price. Detectarea utilizării greșite pe bază de gazdă și colectarea datelor de audit ale sistemelor de operare convenționale lectie. Teză de master, Universitatea Purdue, Purdue, IN, decembrie 1997.

[44] Thomas H. Ptacek și Timothy N. Newsham. Inserarea, evaziunea și refuzul serviciului: eludarea detectării intruziunilor în rețea. Raport tehnic, Secure Networks, Inc., Suite 330, 1201 5th Street SW, Calgary, Alberta, Canada, T2R-0Y6, ianuarie 1998.

[45] Marcus J. Ranum, Kent Landfield, Mike Stolarchuk, Mark Sienkiewicz, Andrew Lambeth și Eric Wall. Implementarea unui instrument generalizat pentru monitorizarea rețelei. În Proceedings of the Eleventh Systems Administration Conference (LISA '97), San Diego, CA, octombrie 1997.

[46] P. Rolin, L. Toutain și S. Gombault. Sondă de securitate a rețelei. În CCS'94, Proceedings of the 2nd ACM Conference on Computer and Communication Security, paginile 229–240, noiembrie 1994.

[47] David R. Safford, Douglas Lee Schales și David K. Hess. Pachetul de securitate tamu: un răspuns continuu la intrușii de pe internet într-un mediu academic. În Proceedings of the Fourth USENIX Security Symposium, paginile 91–118, Santa Clara, CA, octombrie 1993.

[48] Warren S. Sarle. Rețele neuronale și modele statistice. În Proceedings of the Nineteenth Annual SAS Users Group International Conference, aprilie 1994, paginile 1538–1550, Cary, NC, aprilie 1994. Institutul SAS.

[49] Secure Networks, Inc. Sistem de audit al securității Ballista. Internet http://www.securenetworks.com/, 1997.

[50] Stephen Smaha. Haystack: Un sistem de detectare a intruziunilor. În Securitatea informatică a patra aerospațială Conferința de aplicații, paginile 37–44, octombrie 1988.

[51] Steven R. Snapp, James Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che lin Ho, Karl N. Levitt, Biswanath Mukherjee, Stephen E. Smaha, Tim Grance, Daniel M. Teal și Doug Mansur. DIDS (sistem de detectare a intruziunilor distribuite) - motivație, arhitectură și un prototip timpuriu. În Proceedings of the 14th National Computer Security Conference, paginile 167–176, Washington, DC, octombrie 1991.

[52] Michael Sobirey. Bibliografia sistemului de detectare a intruziunilor. Internet: http://www-rnks.informatik.tu-cottbus.de/sobirey/ids.html, martie 1998.

[53] Paul Spirakis, Sokratis Katsikas, Dimitris Gritzalis, Francois Allegre, John Darzentas, Claude Gigante, Dimitris Karagiannis, P. Kess, Heiki Putkonen și Thomas Spyrou. SECURENET: Un sistem inteligent de prevenire și detectare a intruziunilor orientat spre rețea. Network Security Journal, 1(1), noiembrie 1994.

[54] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip și D. Zerkle. GrIDS – un sistem de detectare a intruziunilor bazat pe grafice pentru rețele mari. În Proceedings of the 19th National Information Systems Security Conference, 1996.

[55] Stuart Staniford-Chen, Brian Tung, Phil Porras, Cliff Kahn, Dan Schnackenberg, Rich Feiertag și Maureen Stillman. Cadrul comun de detectare a intruziunilor - formate de date. Internet draft-ietf-cidf-data-formats-00.txt, martie 1998. Lucrări în curs.

[56] Departamentul Apărării al SUA. Criterii de evaluare a sistemelor informatice de încredere, august 1983.

[57] HS Vaccaro și GE Liepins. Detectarea activității anormale ale sesiunii de computer. În Proceedings of the 1989 IEEE Symposium on Research in Security and Privacy, paginile 280–289, 1989.

[58] David Vincenzetti și Massimo Cotrozzi. Atp – program anti manipulare. În Proceedings of the Fourth USENIX Security Symposium, paginile 79–89, Santa Clara, CA, octombrie 1993.

[59] WheelGroup Corporation. Broșura sistemului de detectare a intruziunilor netranger. Internet http://www.wheelgroup.com/.