ATLAS

Framework de securitate
bazat pe metode formale
și învățare automată

RIVER

Detecție de vulnerabilități bazată pe analiză **dinamică**

RIVER este o soluție care detectează vulnerabilități în fișiere binare. Metoda de testare constă în alegea unei intrări aleatoare și rularea programului pe respectiva intrare (testare de tip fuzz).

- *Analiză dinamică de tip taint*. RIVER poate marca părțile din intrare care au fost folosite în timpul execuției.
- *Sistem de execuție simbolică*. Folosind modulul de execuție simbolică a RIVER, împreună cu programul Z3, se pot explora mai ușor diferite căi de execuție ale programului.
- *Sistem de execuție concolică*. Din cauza limitărilor execuției simbolice, aceasta se poate combina cu execuția concolică pentru rezultate mai bune.

Analiza codului binar x86, codul sursă poate lipsi

Algoritmi de inteligență artificială

MALID

Detecție de malware bazată pe analiză **statică**

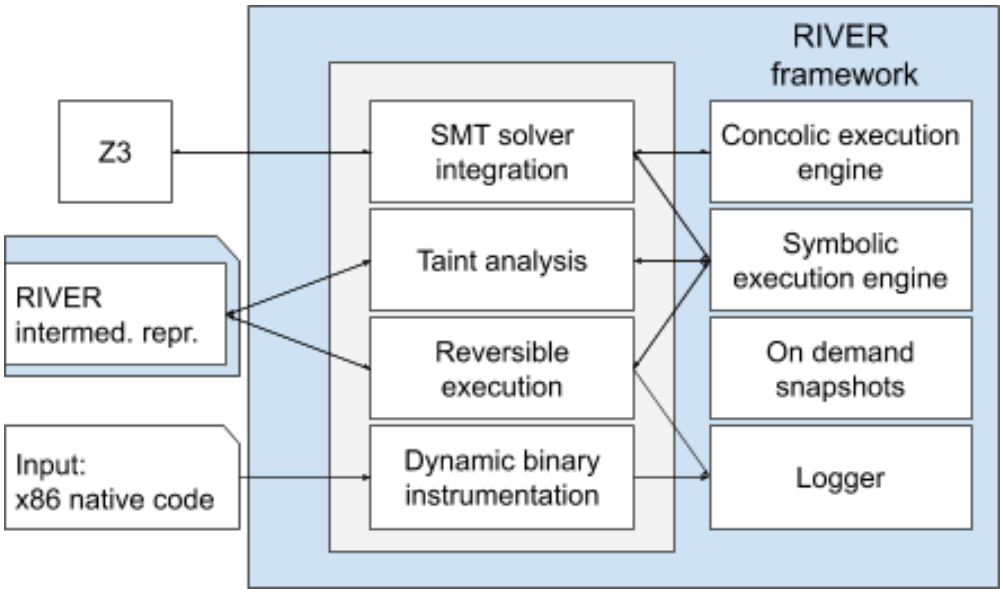
MALID este o soluție de învățare automată (*Machine Learning* - ML) de complexitate redusă bazată pe o metodă de antrenare a dicționarelor (Dictionary Learning - DL), ce poate gestiona colecții din ce în ce mai mari de fișiere.

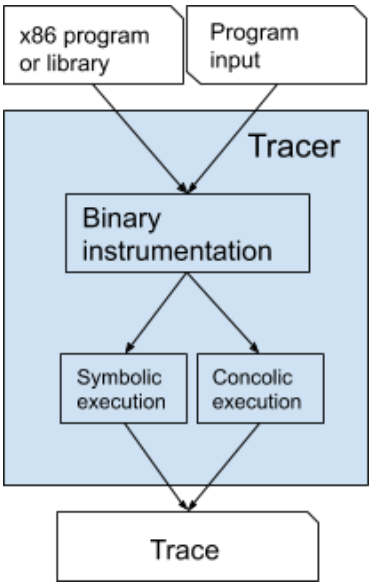
- *Semi-supervizată*. Soluția include o fază inițială de antrenare supervizată ce necesită o bază de date de mici dimensiuni. Cea de-a doua etapă se realizează online. O dată ce un fișier a fost clasificat este ulterior utilizat pentru a reantrena modelul, crescând astfel baza de cunoștințe.
- *Online.* Antrenarea nesupervizată se realizează pentru fiecare fișier separat, ceea ce se traduce într-un update rapid și incremental al modelul.

Model lightweight, complexitate redusă

Adaptiv la noi tipuri de malware

RIVER





Cum funcționează

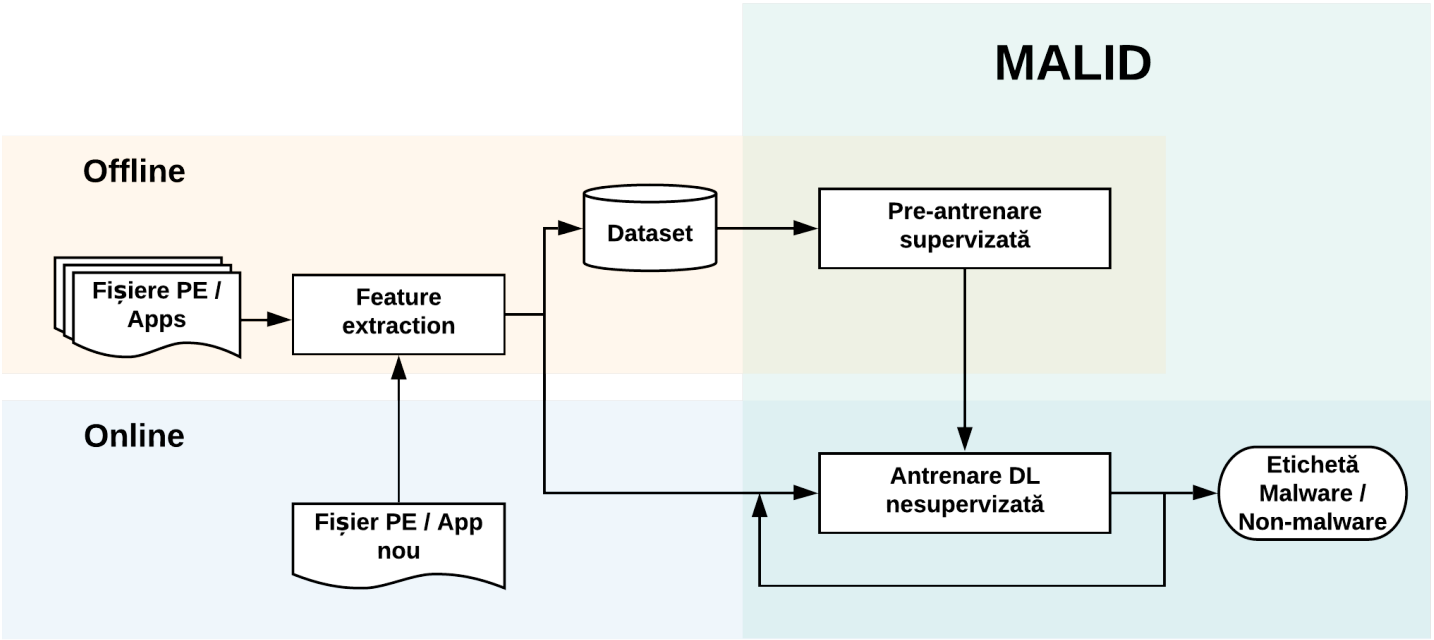
Pentru a folosi soluția RIVER, utilizatorul trebuie să furnizeze un fișier binar de tip x86 sau o librărie. În plus, acesta trebuie sa definească o funcție de tip wrapper pentru a specifica funcția ce trebuie testată. După acest pas se pot aplica mai mulți algoritmi pentru a găsi intrările problematice care produc erori (de exemplu: segmentation fault-uri, hang-uri - timeout-ul este setat manual - sau semnale - sigfpe, sigint, sigabrt etc.).

Programul principal (numit river.tracer) primește o intrare și începe urmărirea execuției programului. Acesta folosește instrumentarea dinamica a fisierului binar pentru a dezasambla codul x86 și apoi de a-l reasambla, modificând condițiile de tip jump astfel încât acesta să apeleze funcții speciale atunci când se executa codul.

În timpul executiei, programul produce o urmă care poate fi examinată pentru a vedea care au fost instrucțiunile care au fost executate. De asemenea, un algoritm poate modifica intrarea pentru a avea o acoperire mai bună a codului.

Pachet software disponibil la: `https://github.com/AGAPIA/river`

MALID



Cum funcționează

Fișierele Portable Executable (PE files) sau descrierile aplicațiilor mobile sunt transformate într-o colecție vectorizată de caracteristici. Un model preliminar de clasificare este antrenat în manieră supervizată pe un set redus de fișiere. După aceasta, fiecare fișier nou ce trebuie clasificat participă la etapa nesupervizată. Aici primește eticheta malware / non-malware și împreună cu aceasta este utilizat pentru a reantrena modelul. Astfel se asigură adaptabilitatea acestuia la tipuri noi de malware. Cum noile fișiere pot influența performanța, un parametru denumit factor de uitare permite controlul senzitivității la noile exemple.

Metoda, Tolerant Online Discriminative DL with Regularization (TODDLeR), extinde un algoritm existent de DL prin includerea a doi factori de regularizare Tikhonov ce asigură faptul că modificările modelului de la un pas la altul se realizează în mod controlat.

Pachet software disponibil la `https://github.com/abaltoiu/malid`

Despre ATLAS

Proiectul “Hub inovativ pentru tehnologii avansate de securitate cibernetică (ATLAS)” își propune îmbunătățirea performanțelor de cercetare și de colaborare în domeniul securității cibernetice, adresând teme de mare interes: securitatea aplicațiilor și sistemelor de operare, securitatea IoT și cloud. Proiectul ATLAS este finanțat printr-un grant acordat de Ministerul Cercetării și Inovării din România, CCCDI - UEFISCDI, proiect nr. PN-III-P1-1.2-PCCDI-2017-0272, în cadrul PNCDI III.