

Academia Tehnica Militara

Sandbox (computer security)

Profesor: Studenti:

Radu Velea Lixandra Bogdan

Filip Catalin

În [securitatea calculatoarelor](https://en.wikipedia.org/wiki/Computer_security" \o "Securitatea calculatorului) , un "sandbox" este un mecanism de securitate pentru separarea programelor care rulează, de obicei în efortul de a atenua eșecurile sistemului sau vulnerabilitățile software. Este adesea folosit pentru a executa programe sau coduri netestate, eventual de la utilizatori sau site-uri nesigure, fără a risca să dăuneze mașinii gazdă sau [sistemului de operare](https://en.wikipedia.org/wiki/Operating_system" \o "Sistem de operare) .

Accesul la rețea, capacitatea de a inspecta sistemul gazdă sau de a citi de la dispozitivele de intrare sunt de obicei nepermise sau restricționate foarte mult.

În sensul asigurării unui mediu foarte controlat**, nisipurile** pot fi văzute ca un exemplu specific de [virtualizare](https://en.wikipedia.org/wiki/Virtualization" \o "virtualizare) . Sandboxing este frecvent folosit pentru a testa programele neconfirmate care pot conține un [virus](https://en.wikipedia.org/wiki/Computer_virus) sau alt [cod rău intenționat](https://en.wikipedia.org/wiki/Malware) , fără a permite software-ului să dăuneze dispozitivului gazdă.

**Definiție - Ce înseamnă *Sandboxing* ?**

Sandboxing este un termen de securitate al calculatorului care se referă la momentul în care un program este pus deoparte de alte programe într-un mediu separat, astfel încât, dacă apar erori sau probleme de securitate, aceste probleme nu se vor răspândi în alte zone ale computerului. Programele sunt activate în zona lor separată, unde pot fi lucrate fără a pune în pericol alte programe.   
  
Nisipurile pot arăta ca un mediu de operare obișnuit sau pot fi oase mult mai goale. Mașinile virtuale sunt adesea folosite pentru ceea ce se numește sandbox-uri runtime.

**Techopedia explică *Sandboxing-ul***

Există, de asemenea, modalități de a utiliza sandbox-ul în aplicații. De exemplu, codul discutabil poate fi folosit într-o manieră sigură, cu un cod de certificare. O "dovadă" trebuie să rămână în vigoare pentru a se asigura că codul este relativ sigur de executat. Acest lucru are o asemănare foarte tare cu cheile implicate în criptare pentru a se asigura că un canal de schimb de încredere este îndeplinit.   
  
Există și alte domenii în care poate fi creat un strat de nisip, cum ar fi o bibliotecă setată pentru a permite sandbox-ul prin interceptarea apelurilor. Biblioteca ar putea, de asemenea, să stabilească un strat de nisip în kernel-ul sistemului de operare.   
  
Când utilizați software care nu este de încredere, este esențial să o utilizați într-o zonă cu nisip, astfel încât alte programe, fișiere și aplicații să nu fie compromise.

**Implementari:**

Un sandbox este implementat prin executarea software-ului într-un mediu de sistem de operare restricționat, controlând astfel resursele (de exemplu, [descriptorii de fișiere](https://en.wikipedia.org/wiki/File_descriptor" \o "Descriptor de fișiere) , memoria, spațiul de sistem de fișiere) pe care un proces le poate utiliza.

Exemple de implementări ale sandbox-urilor includ următoarele:

* [Google](https://en.wikipedia.org/wiki/Google) Sandboxed API
* Jail ([închisoare](https://en.wikipedia.org/wiki/Operating-system-level_virtualization" \o "Sistem de operare la nivel de virtualizare)) : restricții de acces la rețea și un spațiu de nume al sistemului de fișiere restricționat. Jails sunt cel mai frecvent utilizate în [găzduirea virtuală](https://en.wikipedia.org/wiki/Virtual_hosting" \o "Găzduire virtuală) .
* Executarea bazată pe reguli le oferă utilizatorilor un control deplin asupra proceselor care au început, au dat naștere (prin alte aplicații) sau au permisiunea de a injecta codul în alte aplicații și de a avea acces la rețea, atribuiți sistemului niveluri de acces pentru utilizatori sau programe în conformitate cu set de reguli determinate. De asemenea, poate controla securitatea fișierelor / registrilor (ce programe pot citi și scrie în sistemul de fișiere / registru). Într-un astfel de mediu, virușii și troienii au mai puține posibilități de a infecta un computer. **De [SELinux](https://en.wikipedia.org/wiki/SELinux" \o "SELinux) și [AppArmor](https://en.wikipedia.org/wiki/Apparmor" \o "AppArmor)  cadrele de securitate sunt două astfel de implementări pentru**[**Linux**](https://en.wikipedia.org/wiki/Linux_kernel)**.**
* [Mașinile virtuale](https://en.wikipedia.org/wiki/Virtual_machine)[emulează](https://en.wikipedia.org/wiki/Emulator) un computer complet gazdă, pe care un sistem de operare convențional poate să pornească și să ruleze ca pe hardware-ul actual. Sistemul de operare gazdă rulează fără cutie în sensul că nu funcționează negativ asupra gazdei și poate accesa resursele gazdă numai prin emulator.
* Sandboxing pe gazdele native: Cercetătorii în domeniul securității se bazează în mare măsură pe tehnologiile sandbox pentru a analiza comportamentul malware. Prin crearea unui mediu care imită sau replică desktopurile vizate, cercetătorii pot evalua modul în care malware-ul infectează și compromite o gazdă țintă. Numeroase servicii de [analiză a malware-ului](https://en.wikipedia.org/wiki/Malware_analysis" \o "Analiza malware) se bazează pe tehnologia sandboxing.
* Clientul Native este un sandbox pentru rularea eficientă și sigură a codului C și C++ compilat în browser, independent de sistemul de operare al utilizatorului.
* [Secure Computing Mode (seccomp)](https://en.wikipedia.org/wiki/Seccomp) este un sandbox construit în kernel-ul Linux. Când este activat în strict mode, seccomp permite doar  write(), read(), exit() și  sigreturn() apeluri de sistem.
* [HTML5](https://en.wikipedia.org/wiki/HTML5) are un atribut "sandbox" pentru a fi folosit cu [iframe](https://en.wikipedia.org/wiki/Iframes" \o "IFrame) .
* [Mijloacele virtuale Java](https://en.wikipedia.org/wiki/Java_virtual_machine) includ un sandbox  pentru a restricționa acțiunile codului de neîncredere, cum ar fi un  [Java applet](https://en.wikipedia.org/wiki/Java_applet). .

Un applet Java ar putea să apară într - un cadru al paginii web, o aplicație nouă fereastră sau un instrument de stand-alone pentru applet - uri de testare.

Un applet Java creat ca material demonstrativ suplimentar pentru o publicație științifică (si poza)

Un applet Java care utilizează [accelerația hardware](https://en.wikipedia.org/wiki/Hardware_acceleration" \o "Hardware accelerare) 3D pentru a vizualiza fișierele 3D în [format .pdb](https://en.wikipedia.org/wiki/Protein_Data_Bank_(file_format))descărcate de pe un server (poza 2 3D)

* **.** NET [Common Language Runtime](https://en.wikipedia.org/wiki/Common_Language_Runtime) asigură [securitatea codului de acces](https://en.wikipedia.org/wiki/Code_Access_Security" \o "Cod de acces de securitate) pentru a impune restricții asupra codului nesigur

<https://en.wikipedia.org/wiki/Sandbox_(computer_security)>

<https://en.wikipedia.org/wiki/Sandbox_(software_development)>

<https://blogs.msdn.microsoft.com/ie/2011/07/14/defense-in-depth-locking-down-mash-ups-with-html5-sandbox/>

<https://www.youtube.com/watch?v=AlvWXa_uiZo>