Chroot jail

Octubre 2020

El chroot jail és una tècnica mitjançant la qual es pot executar un procés (i els seus corresponents fills) de forma que es restringeix els fitxers als quals pot accedir. Traduït literalment, es tracta d'engabiar (jail) un procés. Per fer-ho es modifica el directori arrel en el qual s'executa el procés. El procés només podrà accedir als fitxers que es trobin dintre d'aquest directori arrel.

Aquesta eina forma part de l'anomenada virtualització a nivell de sistema operatiu, la qual es basa en restringir l'espai d'usuari en què s'executa un procés (i els seus fills). En aquesta pràctica ens centrarem en la comanda `chroot`, que és una comanda que permet restringir l'espai de disc al qual pot accedir un procés. Aquesta eina va ser introduïda el 1979. Arran de les necessitats de restringir l'espai d'usuari en què s'executaven els processos es van introduir noves eines. Els contenidors es van introduir pel cas de Linux. A la següent pràctica introduirem una altra aplicació, anomenada Docker, que utilitza els contenidors per gestionar i restringir l'espai d'usuari en què s'executen els processos.

1 Experiments amb el Chroot jail

Veiem la utilitat d'aquesta aplicació amb un senzill exemple. Al directori fitxers disposeu d'una aplicació C, `statistics.c`, que permet extreure estadístiques del contingut del fitxer. Fem unes proves

1. Compileu el fitxer i genereu l'executable corresponent.

2. Executeu el programa i observeu el resultat de l'execució.

Observeu que podeu indicar a l'executable qualsevol altre fitxer de text pla que tingueu. Dit d'altre forma, l'executable no té restriccions per analitzar qualsevol fitxer de text que hi ha al sistema de fitxers del disc (al qual tingueu accés).

Us proposem doncs crear una gàbia de forma que l'aplicació només pugui accedir als fitxers de text que hi ha a sota d'un determinat directori. Aquest directori serà la gàbia en què s'executarà l'aplicació, la qual només podrà accedir als fitxers que hi ha a sota d'aquest directori.

Per engabiar una aplicació haurem de fer és copiar a l'interior de la gàbia (el directori) tant l'executable com els fitxers als quals pot accedir!

1. Creeu un directori, per exemple "`gabia`". Dins d'aquest directori posarem tots els fitxers que fan falta.

2. Poseu el fitxer `file.txt` dins del directori "`gabia/data`".

3. Compileu l'executable i copieu-lo dins del directori "`gabia/bin`".

Perquè l'executable es pugui executar dins de la gàbia cal copiar dins del directori "`gabia`" les llibreries dinàmiques que es carreguen en executar-ho. Per saber quines es carreguen executeu

```
$ ldd ./statistics
linux-vdso.so.1 (0x00007ffec484a000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f1b322f8000)
/lib64/ld-linux-x86-64.so.2 (0x00007f1b32500000)
```

Copieu doncs, dins del directori "`gabia`", els fitxers `libc.so.6` i `ld-linux-x86-64.so.2` en els directoris corresponents (e.g. `/lib/x86_64-linux-gnu/`).

Ja ho tenim tot fet! Per tal d'executar la gàbia hem de fer

```
$ sudo chroot gabia /bin/statistics
```

El `chroot` requereix permisos d'administrador per poder-se executar. La màquina virtual de la qual disposeu ha estat configurada perquè es pugui executar aquesta instrucció sense haver d'introduir la contrasenya d'administrador.

El primer argument a `chroot` és el directori que farà d'arrel de la gàbia. Les aplicacions que s'executin dins de la gàbia només podran accedir ("veure") el que hi ha dins de la gàbia. El segon argument a `chroot` és l'aplicació a executar que, en aquest cas, és "`/bin/statistics`". Observeu com s'especifica el fitxer executable (amb el directori arrel a l'inici!).

Proveu d'executar la instrucció anterior i contesteu a les següents preguntes.

- Pot l'aplicació llegir el fitxer que hi ha a l'interior del directori "`data`"? En cas que no pugui, per què no pot?
- Quin valor ha de tenir la variable FILE al codi C perquè es llegeixi correctament el fitxer? Ho aconseguiu fer posant una ruta completa al fitxer?

2 Exercici

L'entrega d'aquesta pràctica se centra en construir una gàbia que inclogui un grup reduït de binaris de la línia de comandes . En particular, se us proposa:

- La gàbia ha d'incloure només les comandes `bash`, `ls`, `cp` i `rm` així com el binari `statistics` (totes al directori `/bin`) i les dades descrites a la secció 1. Inclogueu les llibreries dinàmiques necessàries perquè aquestes comandes puguin funcionar correctament.
- La gàbia es pot executar amb

  ```
  $ sudo chroot gabia /bin/bash
  ```

  Es recomana generar la gàbia pas a pas: comenceu per copiar a la gàbia els fitxer necessaris per a `bash`; comproveu que funciona[1]. Després continueu amb `ls`, i així successivament.

[1] Observareu que el bash té un comportament "estrany" el polsar tecles com la de "Suprimir". Això és deu a la configuració local del teclat. Per arreglar-ho caldria copiar dins de la gàbia els fitxers necessaris. En aquesta pràctica no entrarem en aquests detalls.

- Un cop hagueu generat la gàbia observeu que podreu executar les comandes que heu introduït dins de la gàbia. Proveu d'executar les comandes que hi heu copiat a l'interior, així com l'executable `statistics`. Comproveu que no podeu pas veure fitxers fora de la gàbia!

Per sortir de la gàbia cal executar la instrucció `exit`.

3 Entrega de la pràctica

Entregueu la gàbia que heu construït comprimida en format ZIP amb el nombre de la pràctica i grup, seguit del nom i cognom dels integrants del grup:

(e.g. **P1_Grup7_nom1_cognom1_nom2_cognom2.zip**).

Aquesta gàbia haurà de funciona a la màquina virtual que s'utilitza a l'assignatura. Caldrà incloure també al ZIP un informe sobre la feina feta i les respostes a les preguntes realitzades a l'enunciat. L'informe a entregar ha d'estar en format `PDF` o equivalent (no s'admeten formats com `odt`, `docx`, ...). Aquest informe ha de mostrar, de forma resumida, els passos que s'han seguit per construir la gàbia així com les proves que s'han realitzat per assegurar el bon funcionament de la gàbia. En cas que no us funcioni la gàbia indiqueu també el problema detectat així com possibles sospites de quin pot ser la font del problema. Sigueu breus i clars a les vostres respostes, no fa falta que us esteneu en el text escrit.

Inclogueu, preferentment en format text, la comanda que heu executat i algun comentari breu descrivint el resultat si ho creieu necessari. En cas que preferiu incloure captures de pantalla en comptes d'incloure el resultat en format text, assegureu-vos que el text de la captura es pot llegir bé (és a dir, que tingui una mida similar a la resta del text del document) i que totes les captures siguin uniformes (és a dir, que totes les captures tinguin la mateixa mida de text).

Els pesos de la pràctica són: 30% per a la gàbia construïda, 60% per a l'informe entregat. El document ha de tenir una llargada màxima de 4 pàgines (sense incloure la portada on s'inclou el nom dels membres del grup). El document s'avaluarà amb els següents pesos: proves realitzades i comentaris associats, un 60%; escriptura sense faltes d'ortografia i/o expressió, un 20%; paginació del document feta de forma neta i uniforme, un 20%.