Sandboxes

Ambrož Janc

Kaj je sandbox?

- Sandbox je testno okolje, ki izolira izvajanje nove kode od produkcijskega okolja ali repozitorija
- Sandbox je izolirano testno okolje, ki uporabnikom dovoli zaganjati programe, ne da bi tej vplivali na aplikacijo, sistem ali platformo na kateri so zagnani
- Sandbox je fleksibilno varnostno okolje, ki je namenjeno izboljšavi varnosti katerekoli apliakcije
- Sandbox je enkapsulacijski mehanizem, s katerim vsiljujemo varnostna načela

Različne vrste sandboxov

- Na nivoju OS (PyPy, VMWare, Virtualbox):
  - Polno posnemanje sistema (Full system emulation)
  - Posnemanje operacijskega sistema (Emulation of operating systems)
  - Virtualizacija (Virtualization)
- Na nivoju kode (PySandbox, spletni prevajalniki kode)

Kako sandbox deluje?

- Na nivoju OS/hardware:
  - Omejevanje sistemskih virov (dovolimo uporabniku le 20% RAM ali 10% CPU)
  - Omejevanje sistemskih klicev (ne dovolimo klicev kot so fork(), exec(),...)
  - Omejevanje pravic (branje, pisanje, brisanje,...)
- Na nivoju kode
  - Omejevanje funkcijskih klicev (prepovemo klice kot so file(), open(),...)
  - Omejevanje možnih knjižnic (prepovemo knjižnice kot so util, stats,...)
  - Omejevanje možnih podatkovnih tipov (prepovemo uporabo int, boolean,...)
  - Omejevanje konstant (prepovemo uporabo true, false,...)

Uporaba sandboxov v praksi

- Spletni brskalniki
- Android, iOS
- Java
- Windows Sandbox
- PDF bralniki (Adobe Reader)
- Windows, macOS

Sandbox v Javi

- Namenjen varnemu izvajanju kode pridobljene iz nevarnih virov
- Vsak razred dobi svoj zapis kode, ki pove iz kje koda izhaja in njena dovoljenja
- Vsi razredi, ki niso iz lokalnega sistema se privzeto zaženejo v sandboxu
- S sandboxom v Javi upravljamo s security managerjem

```
System.setSecurityManager(new SecurityManager());

System.setSecurityManager(null);
```

Viri

- https://www.cs.cmu.edu/~mmaass/pdfs/dissertation.pdf
- https://khamidou.com/sandboxing/ (https://seccomp-eval.herokuapp.com/)
- https://techcommunity.microsoft.com/t5/windows-kernel-internals/windows-sandbox/ba-p/301849
- https://searchsecurity.techtarget.com/definition/sandbox
- https://www.baeldung.com/java-security-manager
- https://www.howtogeek.com/169139/sandboxes-explained-how-theyre-already-protecting-you-and-how-to-sandbox-any-program/