Pysandbox

Failures and lessons learnt

What is a sandbox

Pysandbox: How it started

2010: Tav: safelite.py

June 2010: Victor Stinner : pysandbox 1.0

September 2010: first vulnerability

Pysandbox: bug and fixes

Modify __builtins__ to change sandbox functions

Blacklists of some dictionnary's instructions (eg: dict.pop(), del dict[key])

Modification of __builtins__ still possible via dict.__init__()

Block access to dict.__init__()

...

Pysandbox: Unusable

- Deny access to the file system
- Deny importing Python modules
- Deny exiting Python
- Deny access to stdin, stdout or stderr
- Deny some builtins symbols like execfile(), reload() or KeyboardInterrupt
- Deny execution of arbitrary bytecode (creation of arbitrary code object)

Pysandbox: Unusable

- Deny access to function closure, globals, defaults and code
- Deny access to frame locals, globals and previous frame
- Deny access to traceback frame
- Deny access to types subclasses
- __builtins__ is read only
- Deny access to dict methods able to modify a dict, eg. dict.__setitem__. But you can use "d[key] = value" and "del d[key]" instead

Pysandbox: How it ended

12 Nov 2013: Victor Stinner : python-dev :

“I am convinced that pysandbox is broken by design”

“The problem is that after each release it becomes harder to write Python code in the sandbox.”

“In my opinion, the compile() vulnerabilty is the proof that it is not possible to put a sandbox in CPython”

“There are too many ways to escape the untrusted namespace using the various introspection features of the Python language”

“For something more complex than evaluating "1+(2*3)", pysandbox cannot be used in practice, because of all these protections”

SECCOMP

- Sandboxing mechanism integrated in the linux kernel (>2.6.12)

- exit
- sigreturn
- read (already opened fd)
- write (already opened fd)

```
prctl(PR_SET_SECCOMP, 1);
```

- Chrome / Chromium (FlashPlayer, Renderer)
- vsftpd
- OpenSSH

Another alternative

Pypy’s sandbox

Resources

- https://lwn.net/Articles/574323/
- https://lwn.net/Articles/332974/