ptrace で実行時プロセス書き換え

hiromi_mi

2022/3/30

概要

- 実行中のプロセス/カーネルを動的に書き換えたい
- Linux カーネルでは実際に使われている
- 一方 ユーザーランドプロセス向けは少ない [1] [2] [3]

- 実行中のプロセスを ptrace を使って 別の関数に置き換えるプログラムを作成した

[1] Fumitoshi UKAI, livepatch - Live Patching for Linux. http://ukai.jp/Software/livepatch/

[2] CGL3.0の実現に向けた Live Patch機能の実装, https://osdn.co.jp/event/kernel2004/pdf/C02.p

[3] libpulp – GitHub, https://github.com/SUSE/libpulp

方針

次の例をもとに方針を紹介する:

実行中のプロセス A の func2() を
別のバイナリファイル B が func3() に置き換える

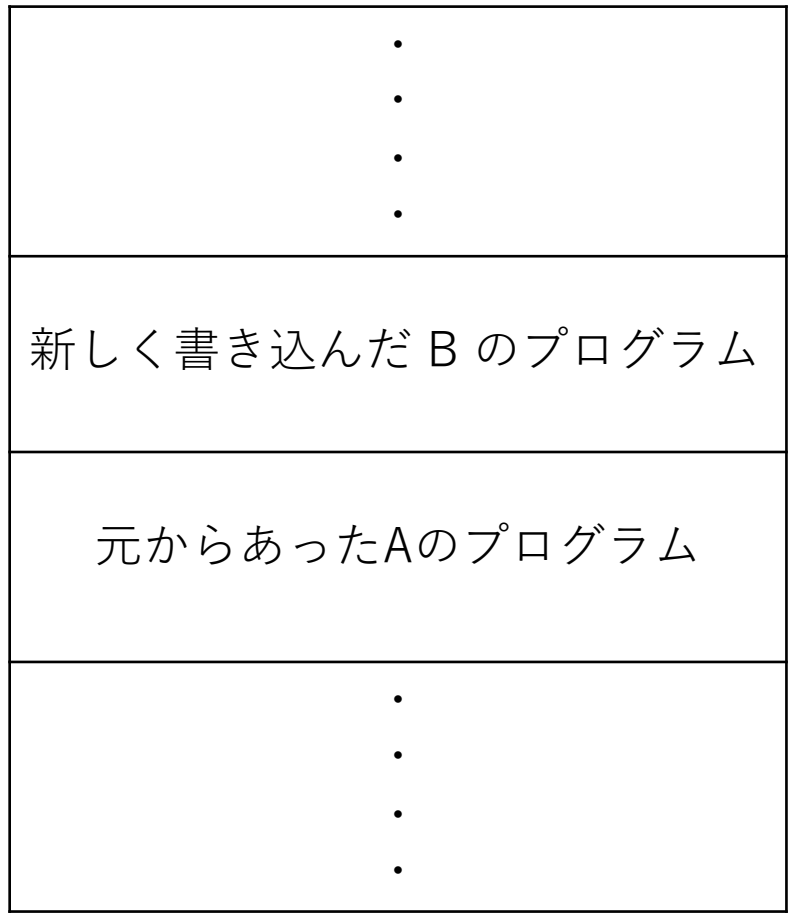
条件としては以下の通り:

- func3() が呼び出す標準Cライブラリの関数は A で使われているもののみ
- ASLR 無効

[1] Fumitoshi UKAI, livepatch - Live Patching for Linux. http://ukai.jp/Software/livepatch/

プログラムの動作

1. 実行中のプロセス A に ptrace (2) でアタッチ
   - Aのメモリやレジスタを操作できる
2. mmap (2) を A に呼び出させメモリ確保
3. ptrace を使い呼び出させるバイナリファイル B を丸ごと A のメモリ空間にコピー



プログラムの動作

GOT (Global Offset Table): 標準関数のアドレスを管理するテーブル

4. B の GOTを A の GOT に書き換える

    これで puts が正しく呼び出せるようになる

5. func2() の先頭を書き換える

    call <func3の相対アドレス>

6. プロセスAからデタッチ