Projekt PaX

- Łata na jądro systemu operacyjnego Linux
- Strona projektu: pax.grsecurity.net

Główne rodzaje ataków związane z błędem przepełnienia bufora

- Niebezpieczeństwa mają źródło w błędach popełnianych przez programistę
- Główne rodzaje ataków polegają na:
  - (1) wprowadzeniu i wykonaniu dowolnego kodu
  - (2) wykonaniu kodu już istniejącego, ale w nieodpowiedniej kolejności
  - (3) wykonaniu istniejącego kodu w oryginalnej kolejności, ale na podmienionych danych

- PaX stara się chronić komputer przed tymi rodzajami ataków
- Jego działanie opiera się na:
  - Uniemożliwieniu wykonania kodu, który znajduje się w obszarze pamięci przeznaczonym na dane
  - Uniemożliwieniu zapisu do obszarów pamięci, które są przeznaczone na kod wykonywalny
  - Losowym rozmieszczeniu obszarów pamięci w przestrzeni adresowej procesu

Ochrona kodu wykonywalnego (Executable Space Protection)

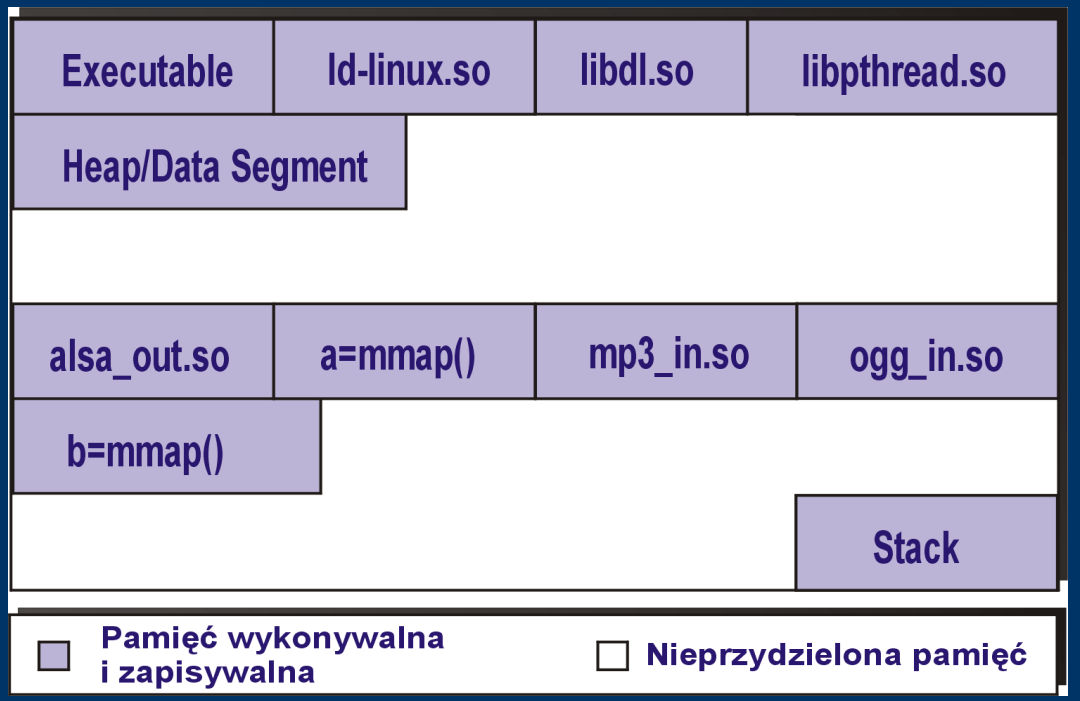
- Oznaczenie każdego obszaru pamięci jako obszar wykonywalny albo zapisywalny
- Wykorzystuje bit NX (Non-eXecutable) lub go emuluje

Linux a bit NX

- Domyślnie Linux wykorzystuje bit NX do odpowiedniej ochrony pamięci
- Proces może zmieniać ustawienia dotyczące swojej przestrzeni adresowej
- Zadanie PaX: uniemożliwienie takich zmian

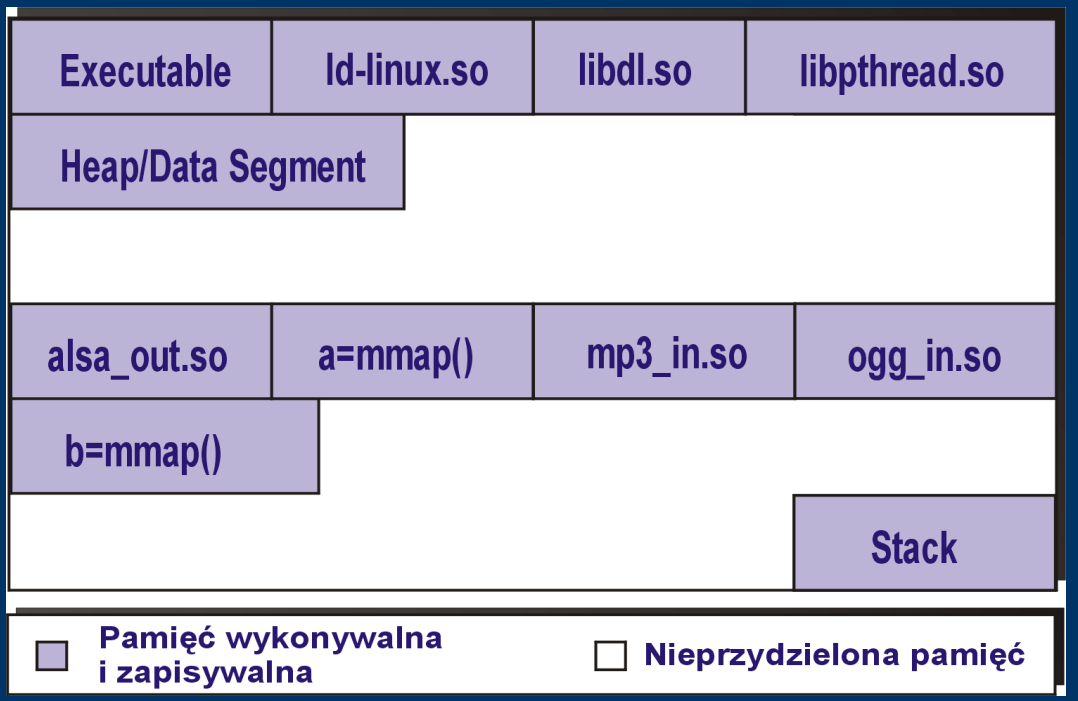
Przestrzeń adresowa procesu bez ESP

- Każdy obszar pamięci w przestrzeni adresowej procesu jest sklasyfikowany jednocześnie jako
  - Zapisywalny
  - Wykonywalny



Przestrzeń adresowa procesu bez ESP

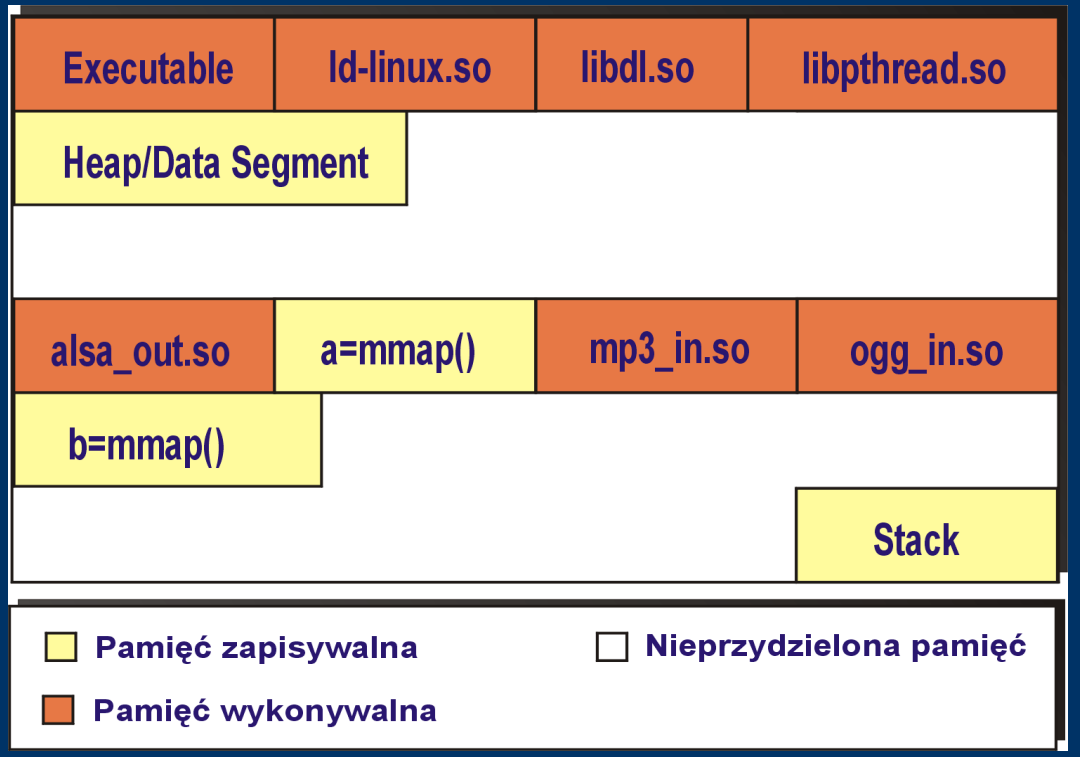
- Każdy obszar pamięci w przestrzeni adresowej procesu jest sklasyfikowany jednocześnie jako
  - Zapisywalny
  - Wykonywalny



Niebezpieczeństwo: możliwość wykonania kodu, który znajduje sie w obszarze pamięci przeznaczonym na dane

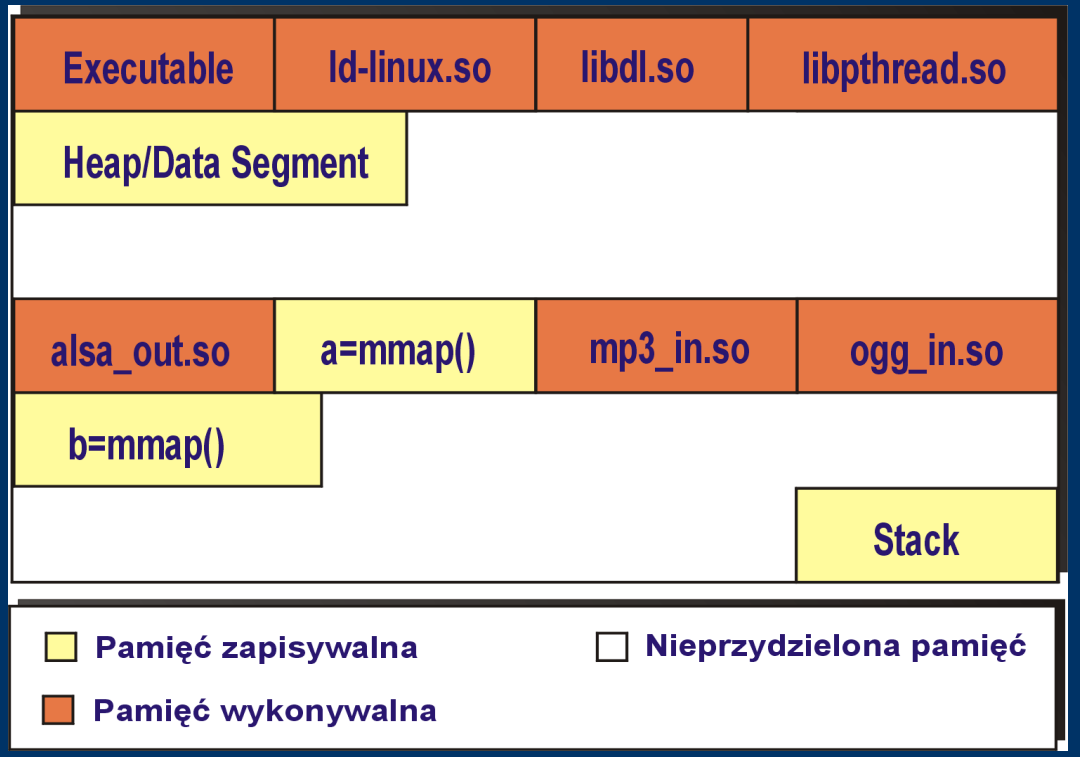
Przestrzeń adresowa procesu z ESP

- Każdy obszar pamięci może być albo wykonywalny albo zapisywalny, ale nie wykonywalny i zapisywalny jednocześnie



Przestrzeń adresowa procesu z ESP

- Każdy obszar pamięci może być albo wykonywalny albo zapisywalny, ale nie wykonywalny i zapisywalny jednocześnie



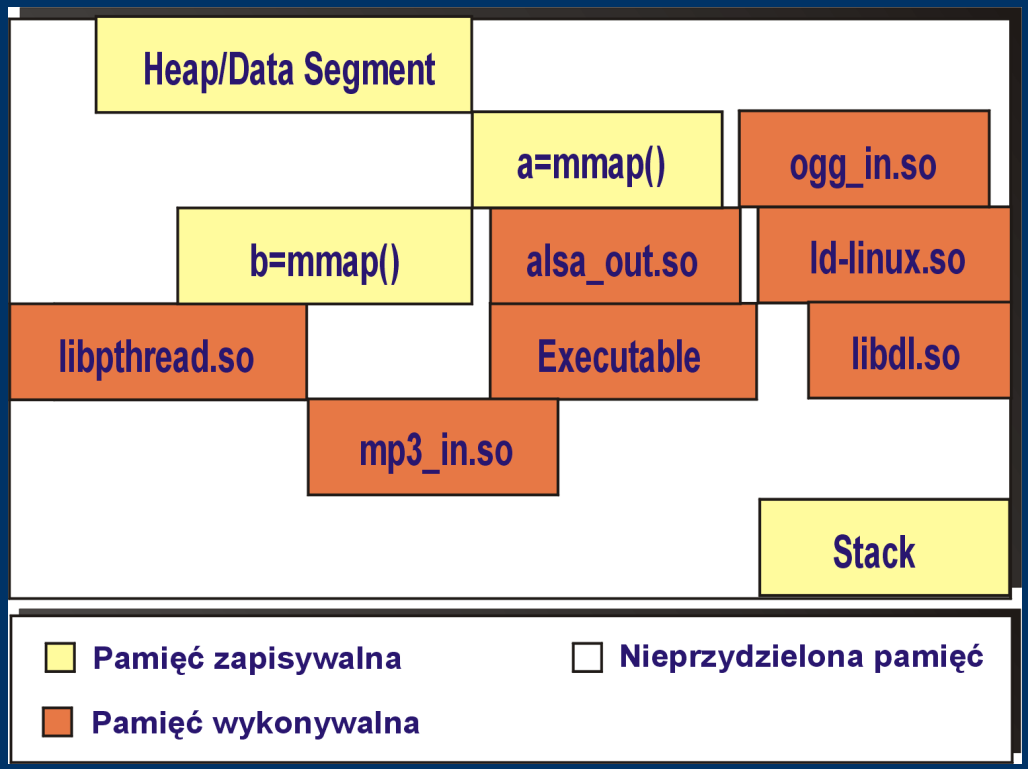
Brak możliwości zapisu do pamięci przeznaczonej na kod oraz wykonywania kodu z pamięci przeznaczonej na dane

Działanie ESP w PaX

- Zapisanie obszaru pamięci uniemożliwia wykonywanie kodu z tego obszaru
- Wykonanie kodu z pewnego obszaru pamięci uniemożliwia późniejsze modyfikowanie tego obszaru
- Zasada minimalnych uprawnień

Randomizacja przestrzeni adresowej procesu

- ASLR – Adress Space Layout Randomization
- Chroni przed atakami, korzystającymi z pewnej wiedzy na temat układu przestrzeni adresowej procesu
- Polega na losowym rozmieszczeniu obszarów w przestrzeni adresowej procesu



Po zastosowaniu ASLR...

- Potencjalny intruz musi “strzelać” w adresy pamięci
- ASLR nie daje 100% pewności bezpieczeństwa – utrudnia ataki i sprawia, że są łatwiej wykrywalne

PaX kontra błąd przepełnienia bufora

- PaX nie jest narzędziem do wykrywania samego błędu. Ma chronić przed skutkami jego wystąpienia
- Główne sposoby wykorzystania błędu przepełnienia bufora:

Podmiana kodu

Podmiana kodu

- Wymaga możliwości zapisu do obszarów pamięci, w których znajduje się kod programu

Podmiana kodu

- Wymaga możliwości zapisu do obszarów pamięci, w których znajduje się kod programu
- Ustawienia PaX gwarantują, że tych obszarów pamięci nie można modyfikować

Podmiana kodu

- Wymaga możliwości zapisu do obszarów pamięci, w których znajduje się kod programu
- Ustawienia PaX gwarantują, że tych obszarów pamięci nie można modyfikować
- Atak kończy się niepowodzeniem

Nadpisanie danych w pamięci, a następnie potraktowanie ich jako kod do wykonania

Nadpisanie danych w pamięci, a następnie potraktowanie ich jako kod do wykonania

- Intruz wpisuje spreparowany kod do odpowiedniego obszaru pamięci

Nadpisanie danych w pamięci, a następnie potraktowanie ich jako kod do wykonania

- Intruz wpisuje spreparowany kod do odpowiedniego obszaru pamięci
- PaX to wykrywa i oznacza ten obszar jako obszar z danymi

Nadpisanie danych w pamięci, a następnie potraktowanie ich jako kod do wykonania

- Intruz wpisuje spreparowany kod do odpowiedniego obszaru pamięci
- PaX to wykrywa i oznacza ten obszar jako obszar z danymi
- Intruz próbuje wykonać wporwadzony kod – próba się nie udaje, atak kończy się niepowodzeniem

Jak dobrze chroni PaX

- 100% ochrona przed atakami polegającymi na wykonaniu podstawionego kodu
- Utrudnienie ataków opierających się na wiedzy na temat przestrzeni adresowej procesu

Jak dobrze chroni PaX

- 100% ochrona przed atakami polegającymi na wykonaniu podstawionego kodu
- Utrudnienie ataków opierających się na wiedzy na temat przestrzeni adresowej procesu – atak jest w 100% skuteczny jeżeli intruz przypadkiem “wstrzeli” się w odpowiednie miejsce pamięci

Wady PaX

- Wykryta próba ataku kończu się “crashem” atakowanego procesu – w niektórych systemach jest to niedopuszczalne
- Niektóre programy wymagają generowania kodu w trakcie działania

Wady PaX

- Wykryta próba ataku kończu się “crashem” atakowanego procesu – w niektórych systemach jest to niedopuszczalne
- Niektóre programy wymagają generowania kodu w trakcie działania – PaX umożliwia administratorowi wyłączenie omówionych wcześniej ograniczeń