SecHack365

KASLR実装に向けて

学習駆動コース　坂井ゼミ　多木 優馬

目標

NetBSDで備えられているPrekernを使って自作OSにKASLRを実装する

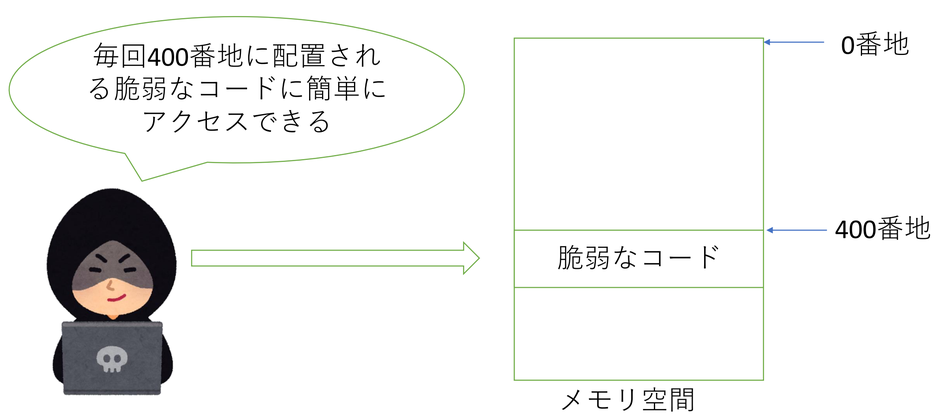
Prekernとは？

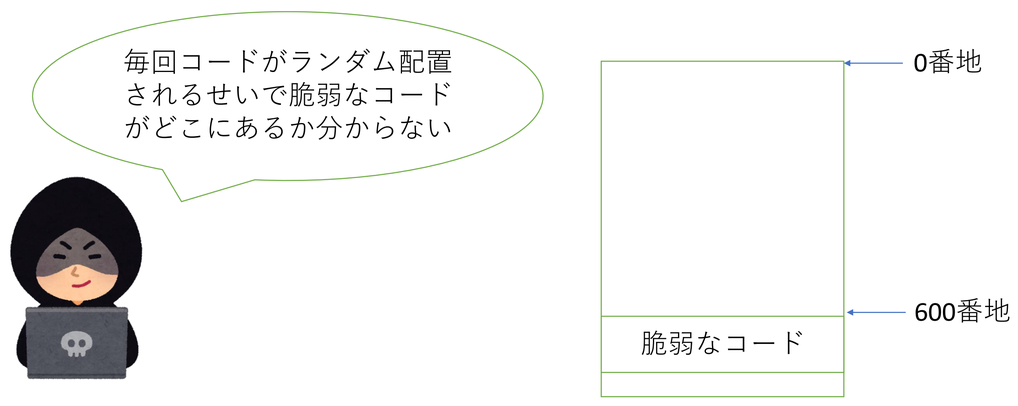
KASLRを有効にするために、カーネルの前に実行される
中間カーネル。メモリとCPUの各種設定を行った後、
カーネルの各セクションの情報を取得し、
ランダムなアドレスにロードした後、
カーネルのエントリポイントにジャンプする。

KASLRとは？

KASLR(Kernel Address Space Layout Randomization)とは、
ブートの度にカーネルのアドレス空間をランダム化して
特定のカーネルデータへのアクセスを困難にするセキュリティ機構。

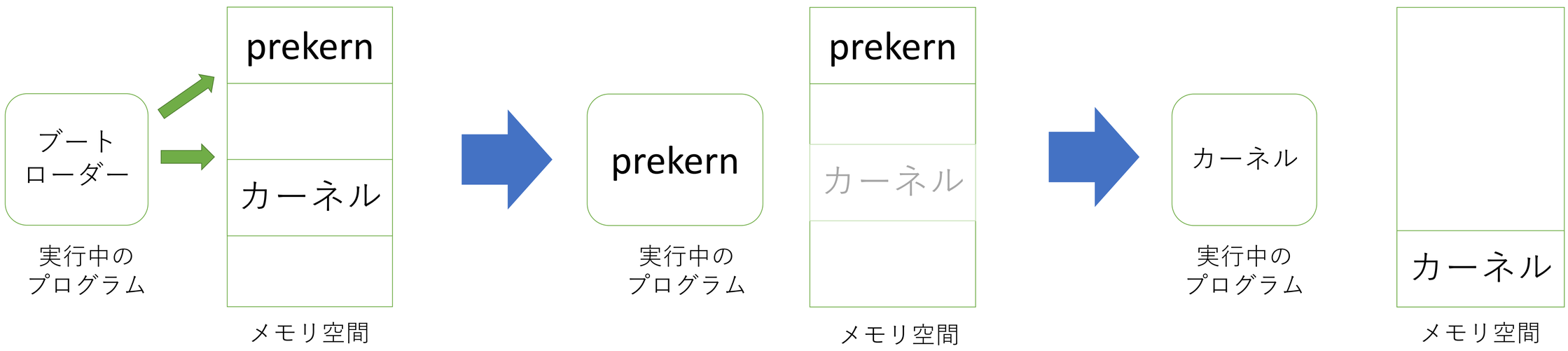
KASLRによる特定のデータへの不正アクセス防止の例





カーネル実行までの流れ

①ブートローダーがPrekernとカーネルをメモリにマップ
②Prekernにジャンプし、メモリとCPUの各種設定を行った後
　カーネルの各セクションの情報を取得し、ランダムなアドレスに再配置
③カーネルにジャンプし、Prekernをメモリから解放する



用意したOS

ブートローダーは”Dragon University2020”を基に、
カーネルは”ゼロからの自作OS入門”を基に実装した。
機能としては、画面出力, メモリ管理のみが実装されている。

実装段階

◎ Prekern(テスト用)とKernelをメモリにマップ

◎メモリやCPUの各種設定

-カーネルの各セクションの情報を取得

-ランダムなアドレスにカーネルを再配置

- カーネルにジャンプ

これまでで実装できたところ

カーネルのELFヘッダからエントリポイントを取得して画面に出力

SecHack365の感想と今後

5月からのOS自作と11月からのPrekernの学習で、
幅広い知識を身に着けることができた。
特にPrekernの学習でELFフォーマットの知識や疑似乱数の生成方法などに触れ、自分の知識が広がっていくのを感じた。
今後もKASLR実装を進め、最終的には実装方法を公開して自作OSブームを更に盛り上げられたらと考えている。

NICT 国立研究開発法人 情報通信研究機構