

WiFi SSID: JP13F
WPA2-PSK (AES)

第8回FreeBSDワークショップ

佐藤 広生 <hrs@FreeBSD.org>

東京工業大学/ FreeBSD Project

2015/6/30

開催背景

- ▶ **日本国内の＊BSD活動は2000年以降、縮小の一途です**
 - ▶ 少なくともユーザ数は大幅に減った
 - ▶ 海外では明るい話題がそれなりにあるのに...
- ▶ 盛り上げたいのはやまやまですが、何をするのが良いですか？

本ワークショップの進行

- ▶ 18:30～19:00 自己紹介＋話題にしたいトピック
- ▶ 19:00～19:30 BSDCan 報告
- ▶ 19:30～19:50 5-6月の変更とSA, EN
- ▶ 19:50～20:00 休憩
- ▶ 20:00～20:30 ライトニングトーク+ α

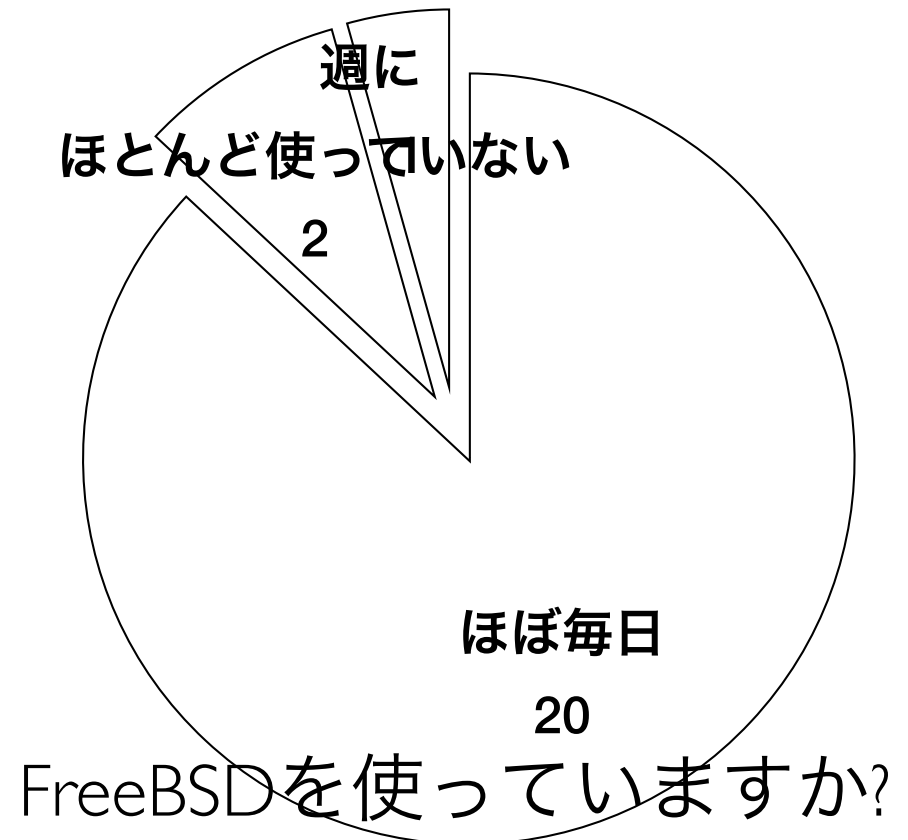
意見は自由に発言ください！

オーガナイザの自己紹介

- ▶ 名前：佐藤 広生
- ▶ FreeBSD コアチームメンバ、リリースエンジニア(2006-)
- ▶ FreeBSD Foundation 理事(2008-)
- ▶ その他の*BSD／オープンソース関連の活動いろいろ
- ▶ 東京工業大学助教(2009-)

自己紹介タイム

- ▶ 名前（所属）
 - ▶ 開発者 or 利用者
 - ▶ 興味がある／話題に
したい内容
- をどうぞ



今回の出席者内訳：新規5名、再参加者18名

✕ 毛

✕ 毛



- ▶ 毎年6月にある*BSD最大のカンファレンス
- ▶ オタワ大学（カナダ）
- ▶ おおよそ200-250名くらい参加。
FreeBSD開発者は半分くらい。



- ▶ FreeBSD Developer Summit (前半2日間)
WGに分かれて議論とハッカソン
適宜プレゼンの時間もとる

- ▶ Talk Session (後半2日間)
一人1時間、2015は4並列トラック
ビデオがYouTubeにあります (※)

※ <https://www.youtube.com/playlist?list=PLWW0CjV-TafY0NqFDvD4k31CtnX-CGn8f>



▶ ハイライト



- ▶ Appleが使っているproplistのように、/etc などにある設定ファイルの書式を統一しようという話。



▶ ハイライト

newsyslog.conf(5) before:

```
/var/log/messages 644 5 100 @0101T JC
```

After:

```
mylogfile: {  
  filename: "/var/log/messages"  
  mode: 644  
  count: 6  
  size: 100kb  
  when: "@0101T" /* this could be written in crontab(5) style? */  
  create = yes  
  compress = xz  
}  
include "/usr/local/etc/newsyslog.d/*.conf"
```

- ▶ Appleが使っているproplistのように、/etc などにある設定ファイルの書式を統一しようという話。
- ▶ 基本的にJSON 形式。
- ▶ libuclとシェルスクリプティング用のユーティリティを開発中。
- ▶ まだ道半ば。



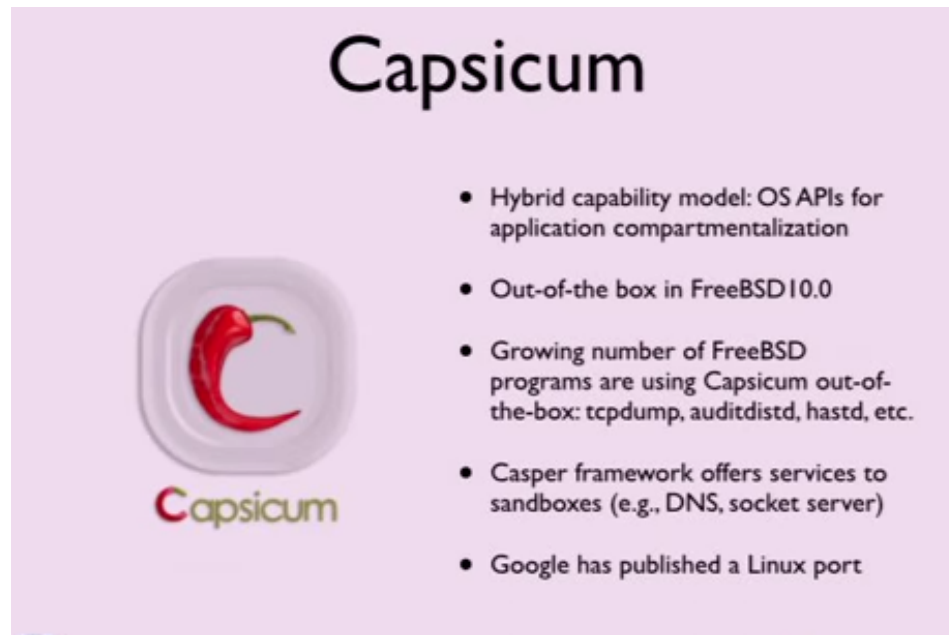
▶ ハイライト



- ▶ DARPA CRASH 研究プログラムにおいて、SRIとケンブリッジ大学が行っている対障害・高機能システムの研究に使っている FreeBSD
- ▶ 既存のUNIXシステムとの互換性を重視しつつ、セキュリティを向上させることが目的。
- ▶ Rethinking the hardware-software interface for security



▶ ハイライト



- ▶ Capsicum: ケーパビリティベースのセキュリティ機構を扱うためのAPI
- ▶ ケーパビリティの機能を、POSIX APIの記述子に持たせる。プロセス記述子を追加。
- ▶ アプリケーションのコンパートメント化



▶ ハイライト

CHERI capabilities

Base [64]		
Length [64]		
Permissions [32]	Type [24]	Reserved [8]
Offset [64]		

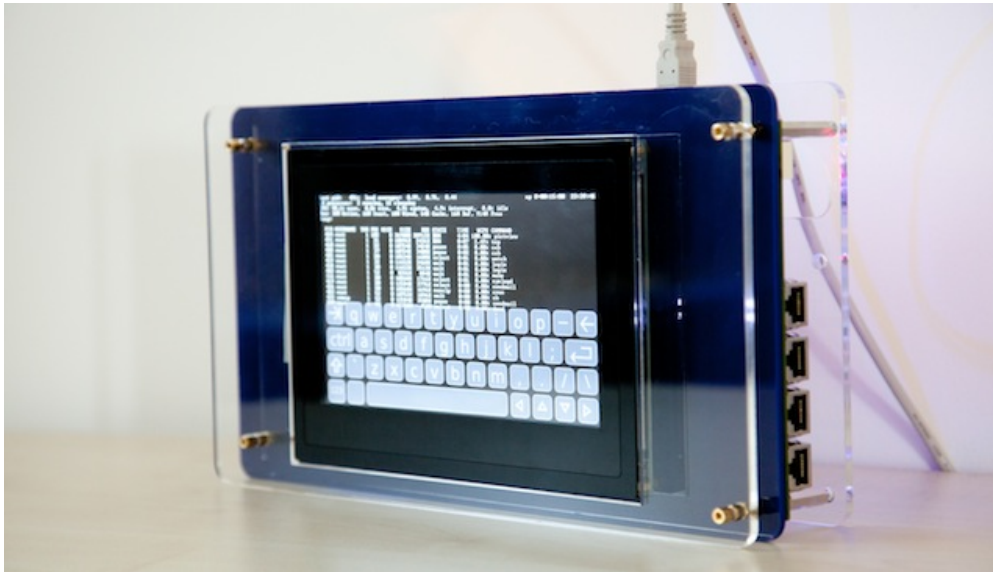
- Unforgeable
- Monotonic length and permissions
- Tagged memory protects capabilities
- Checks apply only on dereference



- ▶ CHERI: Capability Hardware Enhanced RISC Instructions
- ▶ ポインタすべてにカーナビリティの機能を持たせる(fat pointer)
- ▶ アプリケーションの中で、すべてのポインタアクセスがチェックされる。



▶ ハイライト



- ▶ MIPS64 ISA (R4000)を
FPGAで実装し、ハードウェア
レベルでサポート
- ▶ コンパイラはLLVMを使って
拡張
- ▶ CheriBSD:
BERI CPU 上で動作する
FreeBSD/mips + ケーパビリティ
対応の拡張



▶ ハイライト

FreeBSD DCTCP highlight

- ▶ What is the average transmission time of 10 800KB transfers while 2 long flows are running in the same link?
 - ▶ TCP (NewReno): 252.7 msec
 - ▶ DCTCP: 82.5 msec
 - ▶ One-sided DCTCP: 89.4 msec

Using BSD DCTCP achieves faster data transfer than using TCP not only in the fully deployed network but also in the partially deployed network.

- ▶ DCTCP
- ▶ L3SWのECN (RFC3168) を有効にして、スイッチキュー長に応じてECNが出るように設定
- ▶ エンドホストはECNを受け取った時に、TCPウィンドウサイズの減少量をキュー長を考慮して細かく制御する（あまり極端に減らさないようにする）
- ▶ 輻輳制御技術のひとつ



▶ ハイライト

FreeBSD DCTCP highlight

- ▶ What is the average transmission time of 10 800KB transfers while 2 long flows are running in the same link?
 - ▶ TCP (NewReno): 252.7 msec
 - ▶ DCTCP: 82.5 msec
 - ▶ One-sided DCTCP: 89.4 msec

Using BSD DCTCP achieves faster data transfer than using TCP not only in the fully deployed network but also in the partially deployed network.

- ▶ L3SWのバッファがあふれにくくなる（再送が減る）
- ▶ 長時間の大容量トラフィックと、短時間のトラフィックが混在した場合に、短いトラフィックの遅延が増加する現象が緩和される（結果的に速度があがる）
- ▶ スループットと遅延量の変動が非常に小さくなる。



▶ ハイライト

- ▶ QEMU を使って、速いマシンで FreeBSD/arm のパッケージを構築するお話。



**Embedded FreeBSD Development
and Package Building
Via QEMU**

Sean Bruno, sbruno@FreeBSD.org

Stacey Son, sson@FreeBSD.org

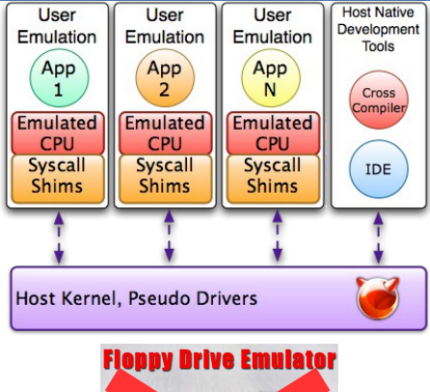


▶ ハイライト



QEMU User Mode Emulation

- **Only CPU is emulated. MMU, I/O, etc. are not.**
- System calls are translated to host calls and/or emulated.
- Can use native host tools for cross development. Cross debugging and testing.

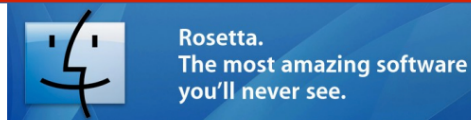
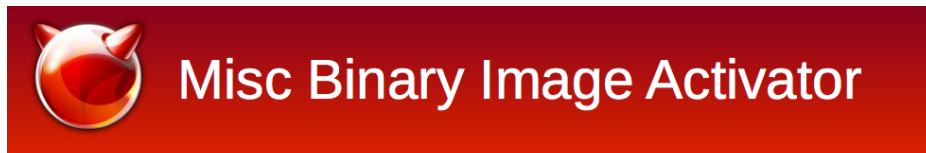


The diagram illustrates the QEMU User Mode Emulation architecture. It shows three vertical columns for "User Emulation", each containing "App 1", "App 2", and "App N". Below each app is a box labeled "Emulated CPU" and "Syscall Shims". To the right of these is a column for "Host Native Development Tools" containing "Cross Compiler" and "IDE". All these components are connected by double-headed arrows to a central purple box labeled "Host Kernel, Pseudo Drivers". Below this box is a red box labeled "Floppy Drive Emulator".

- ▶ QEMU を使って、速いマシンで FreeBSD/arm のパッケージを構築するお話。
- ▶ ユーザモードエミュレーション = CPUだけエミュレーションし、システムコールは変換する。



▶ ハイライト

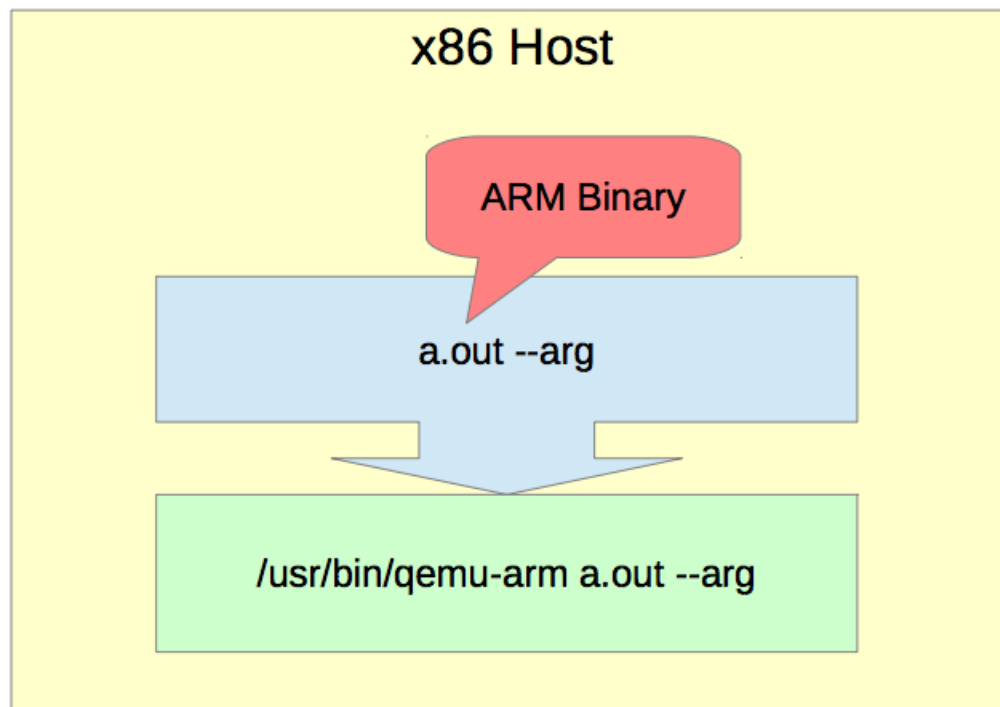


- 'imgact_binmisc.ko' is a kernel image activator that will invoke an user-level emulator or interpreter based the binary header of the file.
- binmiscctl(8) is a command-line utility that is used to load the kernel module (if not already loaded) and configure the interpreter/emulator path for a set of magic bytes and mask.
- Part of FreeBSD since 10.1.

- ▶ QEMU を使って、速いマシンで FreeBSD/arm のパッケージを構築するお話。
- ▶ ユーザモードエミュレーション = CPUだけエミュレーションし、システムコールは変換する。
- ▶ 10.1Rから入った binmisc というimgactを使うと、ユーザレベルエミュレータを使ってバイナリ起動ができる。



▶ ハイライト



- ▶ QEMU を使って、速いマシンで FreeBSD/arm のパッケージを構築するお話。
- ▶ ユーザモードエミュレーション = CPUだけエミュレーションし、システムコールは変換する。
- ▶ 10.1Rから入った binmisc というimgactを使うと、ユーザレベルエミュレータを使ってバイナリ起動ができる。



▶ ハイライト



Current State of QEMU Cross Building

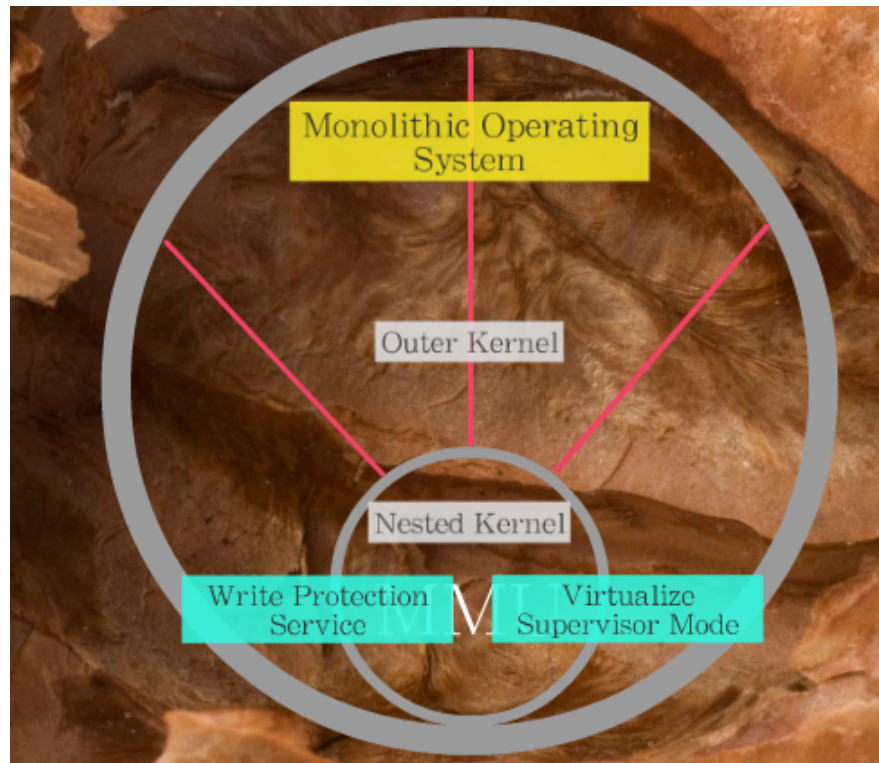
- The ports cluster is building packages for arm, mips, and mips64. Nearly 50,000 packages!
 - Over 20,000 for arm, 15,000 for mips and 12,000 for mips64. (All coming to a pkg.FreeBSD.org near you.)
- Aarch64/ARM64 support is mostly there
 - Have cross built a handful of packages (e.g. vim-lite)
 - Missing some threading/_umtx_op() stuff, etc.
- QEMU- Sparc64 and PPC will run simple static binaries.

<https://wiki.freebsd.org/QemuUserModeHowTo>

<https://github.com/seanbruno/qemu-bsd-user/tree/bsd-user>



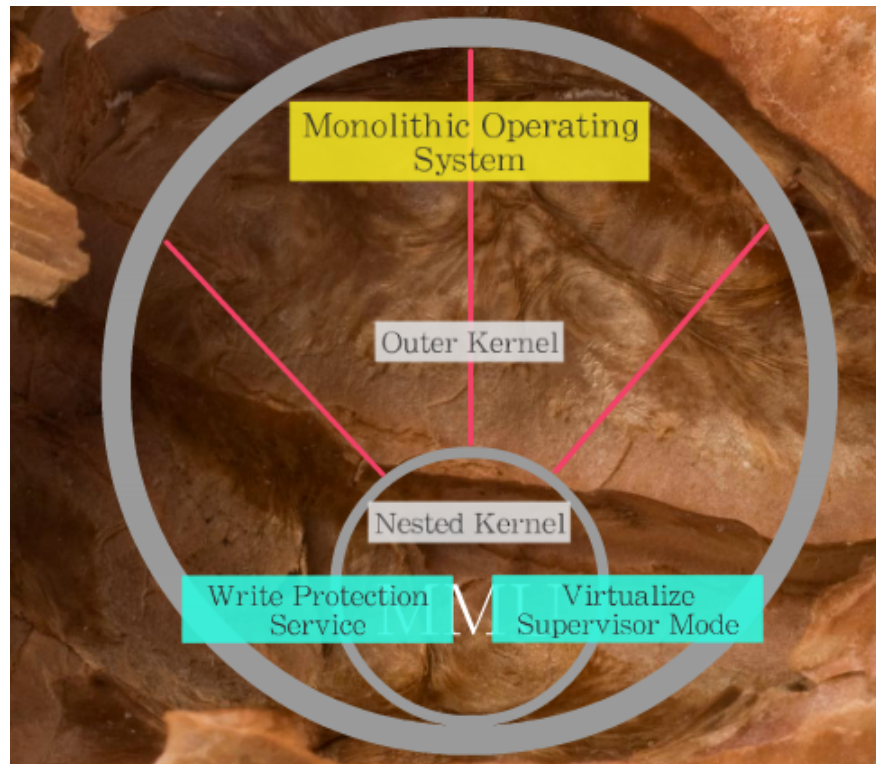
▶ ハイライト



- ▶ Nested Kernel
- ▶ 現在のカーネルでは、
カーネルモードで動作するコードは、
メモリ破壊が容易にできる
- ▶ カーネルページテーブルへのアクセス
を制限
= CR3とPTのメモリ領域を全てRO化
- ▶ PTへの書き込みアクセスを提供するサー
ビスを、スーパーバイザ権限で動作する
コードとしてカーネル内につくる
= CR0 のWP bitを1にしておく



▶ ハイライト

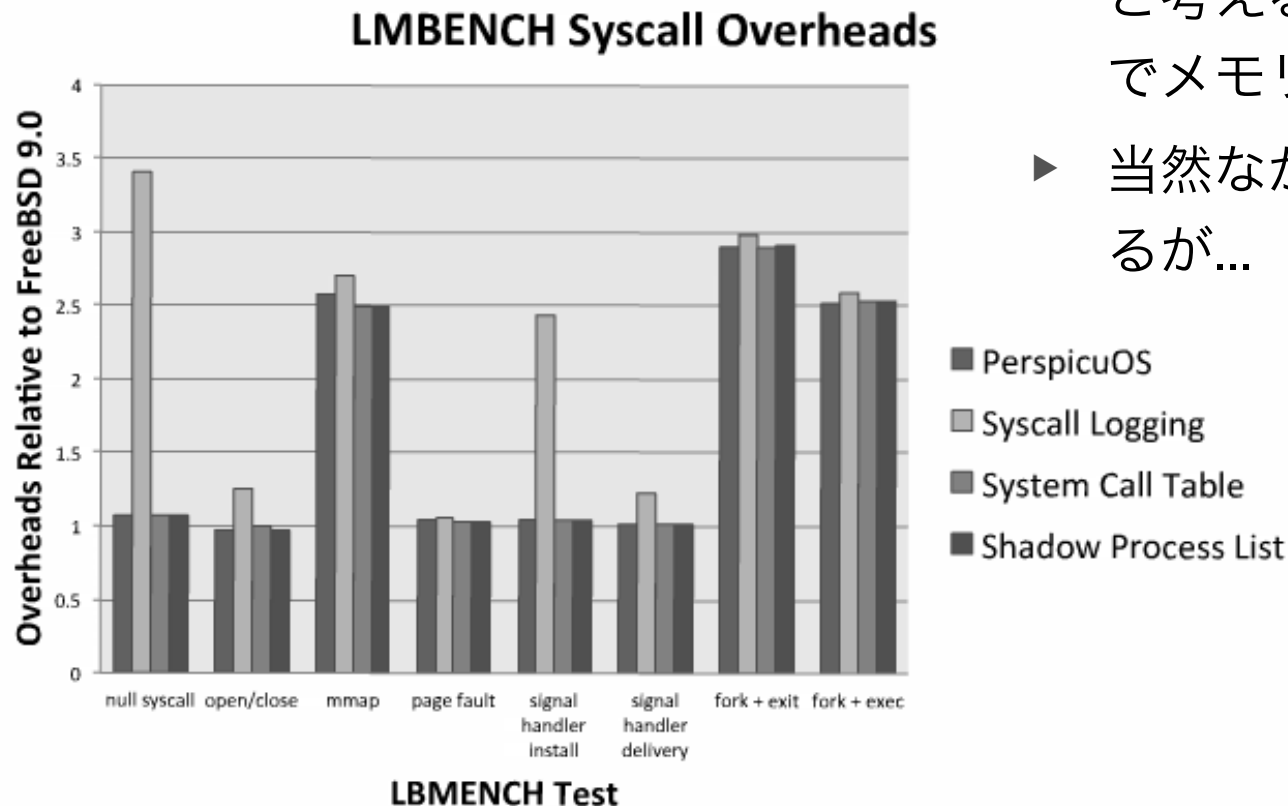


- ▶ PTへアクセスするカーネルコードは、割り込み禁止でMMUの操作のみを行う。
- ▶ それ以外のカーネルコードは、PTの書き込みポリシーに従ってメモリアクセスが制限される
- ▶ CR3 とか CR0 の操作をするコードがあったら？
＝コードを書き換える



▶ ハイライト

- ▶ MMU操作部分をTCBとするカーネルと考えることができ、カーネルコードでメモリ保護ができるようになる
- ▶ 当然ながら mmap() がかなり遅くなるが...



最近の話題

▶ SA

▶ FreeBSD-SA-15:09.ipv6

RAを使うと、ホストのホップリミットを小さく設定できるので、DoSできるじゃん、と言った人がいた。要再起動。

▶ FreeBSD-SA-15:10.openssl

Diffie-Hellman鍵交換の鍵長を512bに落とす攻撃(logjam)。768b 以上じゃないと弾くようになった。再起動不要。

プロトコルスイート: 鍵交換-認証-暗号化-MAC

例) DHE-RSA-AES128-SHA1

(TLSはPerfect Forward Secrecyの目的で DHE or ECDHEを使う)

最近の話題

▶ EN

▶ FreeBSD-EN-15:05.ufs

10.1Rでインストーラを使った場合、freebsd-update直後の再起動で固まる、という話。一度電源ON/OFFすると治る。
SU+J のデッドロック。要再起動。

▶ FreeBSD-EN-15:06.file

file(1)で DoSができる。が、このパッチをあてるとfile(1)が xlocaleを使うようになり、xlocaleのバグを踏んで落ちることが発覚。ただいまxlocaleのEN(15:09)を準備中。
再起動不要。

最近の話題

▶ EN

▶ FreeBSD-EN-15:07.zfs

ZFSのTRIM/UNMAPを使うとたまにパニックすることと、メモリリークを直した。要再起動。

▶ FreeBSD-EN-15:08.sendmail

SA-15:10.opensslのせいで 512b のDHEが使えなくなったのに、sendmail が 512b を使い続けようとする問題。

DHパラメータの再生成も必要。再起動不要。

実はパッチが足りなかったなので、更新されます

最近の話題

- ▶ **EN (まだ出てない)**

- ▶ FreeBSD-EN-15:09.xlocale

setlocale()呼ばないでuselocale()だけでlocale APIを使おう
とすると、EUCなどのエンコーディングでプログラムがクラッ
シュする。

- ▶ FreeBSD-EN-15:10.iconv

UTF-7の処理がおかしいので直した。

おしまい

▶ 質問はありますか？