Портирование Linux на КПК на базе WinMobile

или Коротко о реверс-инжиниринге

Василий «anarsoul» Хоружик

1 – 4 июля / LVEE

Зачем это мне?

- Любимая ОС
- Приобретаемый опыт
- Just for Fun :)

Какая от этого польза для community?

- Тестируется и исправляется код для определённого семейства процессоров
- Новые драйвера (а вдруг кому-нибудь пригодятся? :))

iPAQ RX1950 – что это за зверь?

- Samsung S3C2442 (arm920/32mb RAM/64mb NAND)
- WinMobile 5
- Почти вся периферия в одном чипе (SoC)
- Нет PnP (почти)

- Что это такое?
- Как под WinMobile?

Реверс инжиниринг и WinMobile – как?

- Дизассемблирование частей WinMobile
- Исследование HW (прозвонка GPIO)
- JTAG
- HaRET
- Документация :)

Handhelds Reverse Engineering Tool

- Загрузчик ядра Linux (и не только ядра Linux)
- Инструмент для реверс инжиниринга

HaRET умеет:

- Перехват обращений к памяти и регистрам контроллеров
- Перехват прерываний
- Отслеживание состояний GPIO
- Загрузка Linux и u-boot

Краткая инструкция

- Файл arm-машины
- Составление карты GPIO
- Составление карты прерываний
- Последовательности включения /выключения периферии
- Suspend /Resume
- Драйвера для неподдерживаемой периферии
- Загрузчик

Что сделал я?

- Порт Linux для HP iPAQ RX1950 (почти весь :))
  - Поддержка базовой периферии RX1950 в 2.6.35
  - Работа над включением драйверов батарейки и звука в 2.6.36
- Патчи для HaRET
- Порт u-boot для RX1950 и H1940

Статус

- Сделано
  - Поддержка всего железа на RX1950 (включая звук и WiFi)
  - Suspend /Resume
  - u-boot (можно зашить Linux во внутренний флэш)
  - rootfs с opie (Angstrom)
- Не сделано
  - Документация
  - Полировка до состояния ready for users
  - rootfs с современным софтом

Спасибо за внимание!

Вопросы?