

# Homebrew Gaming Tools

- Joachim "Jok" Thuau
- IT for a small indie studio
- [epac@korigan.net](mailto:epac@korigan.net)

# Homebrew Gaming Tools

Making games on all sorts of game consoles

- Got an idea?
- Got some art/design/programming skills?
- Want to make  $> \$10^6$ ? (maybe?)

# Development options

- Licensed tools / dev hardware
- Non-Licensed tools and retail hardware

# Motivations

- For the Pros?
  - Fame, Money, Fast Cars, Mansion,...
- For the Homebrewer?
  - Linux! (never underestimate the power of large groups of students with nothing but time on their hands!)
  - Cheap way to get familiar with interesting tech

# Hardware for Pros

- Sony licensed hardware, for example (PS2, PS3 and PSP)



# Tools for Pros

- A lot of tools from the embedded community
  - Codewarrior IDE + custom compilers
  - Custom minimal toolchains
- And some not so embedded
  - Visual Studio (Xbox/Xbox360) + SDK

# Pros/Cons

- Made for the hardware, by someone who should know the hardware in and out
- Good docs (most of the time)
- VERY expensive
- NDAs
- Lots of regulation from vendor

# So Homebrew then?

- Hardware is cheap (retail hardware realm)
  - Gamecube (\$40 to \$60)
  - Wii < \$300
  - PSP < \$200

software is free\*, and hardware is really cheap

(\* ) Free (Beer) and/or Libre

# Platforms

- PS3
  - XBOX360
  - Wii
  - PSP
  - DS
  - GBA
  - Gamecube
  - N64/SNES/NES
  - PS2/PS1
  - Dreamcast
  - Genesis/SMS
  - AtariVCS  
(2600/5200/7800)
- Remember those?

# Status of Homebrew today

## Older Consoles

- Atari VCS
- SMS/Genesis/Gamegear
- GB/GBC/GBA
- NES/SNES/N64
  - Writeable cart + reader/writer
  - assembler/libs

# Homebrew, Last Generation

- Dreamcast (no modchip)
  - Run loader from CD, load over network, or load CD
- PS2 (with or without modchip)
  - Load on MC/CD/HDD/ETH
- Xbox (with modchip)
  - Load custom dashboard, Load on internal HDD
- Gamecube (with modchip)
  - Load over ETH(BBA) or from CD (or modchip)

# Portables 1/2

- DS
  - NDS Classic, NDS Lite
  - Writeable cart to put your code on
    - R4DS/CycloDS/EvolutionDS/EdgeDS
  - Compiler/linker/libs
    - DevkitARM (will get to that in a minute)
- The DSI (the new one) is a new beast, above not directly applicable

# Portables 2/2

- PSP
  - Retail PSP, older ones are better (simpler)
  - MSPRO Duo (memory stick)
  - Compiler/linker/libs
    - devkitPSP

# Latest Generation - PS3

- Linux out of the box!
  - Not so motivated to do much with that
  - Hardware access is limited
- There are efforts underway to build a PS3SDK
  - [ps3dev.org](http://ps3dev.org)
- BD-java, which is slow, limited in scope
- HDD is encrypted/signed. Makes it difficult to do much of anything

Homebrew on PS3 = linux or BD-java

# Latest Generation - X360

- Exploit in the Hypervisor
  - Specific to a couple version of the flash
  - OTP bits on CPU, not "downgradable"
  - Hack involving KingKong, modchip, custom shader
  - Allowed development of XeLL (Xenon Linux Loader)
  - No longer working
  - Work in progress on a different type of modchip to load older flash from alternate location

# Latest Generation - Wii

- Memory Probing/dumping via external means
- Undermine security mechanism (common keys)
- Reverse engineering effort leads to loaders
  - Trucha Signer (to generate fake signature on discs)
  - Homebrew Channel (HBC) via exploit on game
  - BootMii (full control of hardware / pre-IOS load)

# Generic Pipeline overview

- Source
- Objects/Libs
- Executable
- Compiler
- Linker
- Loader
- Debugger

# DevkitPro

- DevkitPro
  - Combination of "compiler suite" (ARM/PPC/MIPS)
  - Multiple targets
  - Libs to access hardware

# DevkitPro - devkitARM

- Target: NDS, GBA, GP32
- Libnds: basic hardware, 2D/3D
- Dswifi: access to wifi hardware/network
- Libfat: file access
- Libmaxmod: audio
  
- PALib

# DevkitPro - devkitPPC

- Target: Gamecube, Wii
- Libogc: just about everything Wii/GC  
(video/audio/network/controllers/etc)
- Libfat: filesystem access

# DevkitPro - devkitPSP

- Toolchain packaged from [ps2dev.org/pspdev.org](http://ps2dev.org/pspdev.org)
- Special case
- Includes huge number of tools to work with the PSP (psplink in particular)

# How to install devkitPro

- From Source
  - Download the buildscript from the release, and try to compile it (I have had little success with that)
- Binaries
  - Linux binaries (32/64bit), OSX, win32
  - Download, extract
  - DEVKITPRO/DEVKITARM/DEVKITPPC env

# DEMO

- **WII**
  - Setting up a retail Wii with HBC/bootmii
  - Setup on dev (and tools)
  - Running examples
- **DS**
  - Running the examples
- **Starting a new project**
  - Templates available

# Questions ?

# Links

- DevkitPro: [www.devkitpro.org](http://www.devkitpro.org)
- Wii tools:
  - BootMII homepage: [www.bootmii.org](http://www.bootmii.org)
  - Homebrew Channel: [hbc.hackmii.org](http://hbc.hackmii.org)
  - Docs: [www.wiibrew.org](http://www.wiibrew.org)
- Downloads: [devkitpro.sourceforge.net](http://devkitpro.sourceforge.net)

**Thank you**