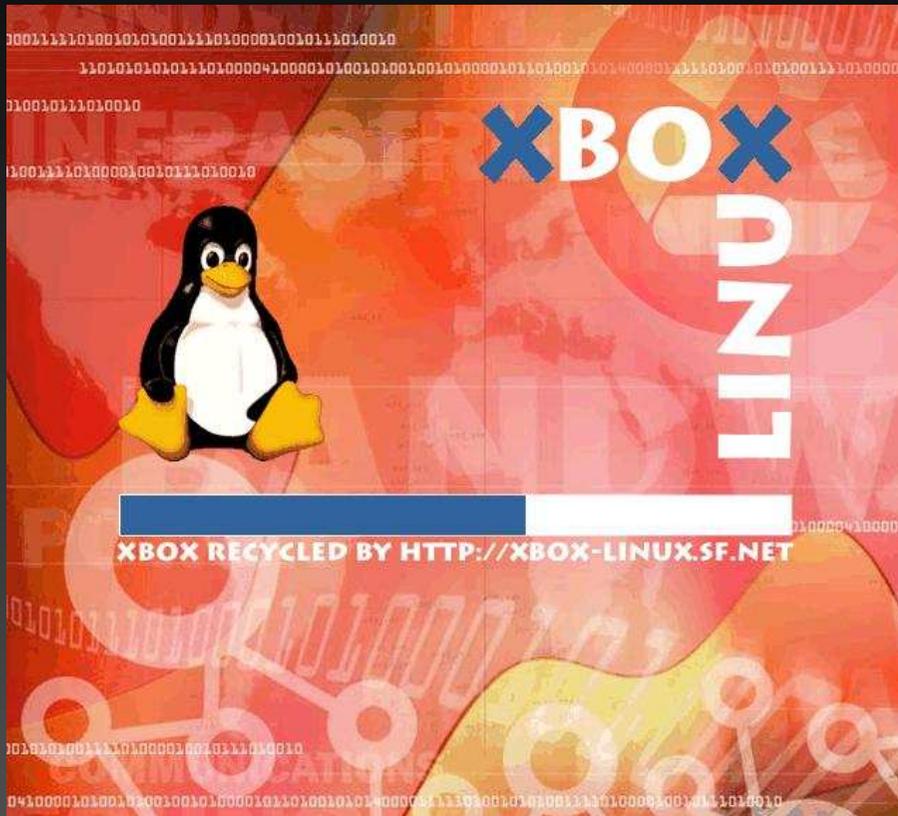


Xbox meets linux



Xbox meets linux



LugBE Offevent
18.9.2003
Restaurant Beaulieu

Marc Herren

maildrop@dj-submerge.c



**It's "Unix" if it has the "x" source
name - the Xbox must be Unix**

From a discussion on slashdot.c



Overview

What is the Xbox ?

Hardware modification

Exchange the bios

Install / run linux

Practical use

What is the Xbox ?

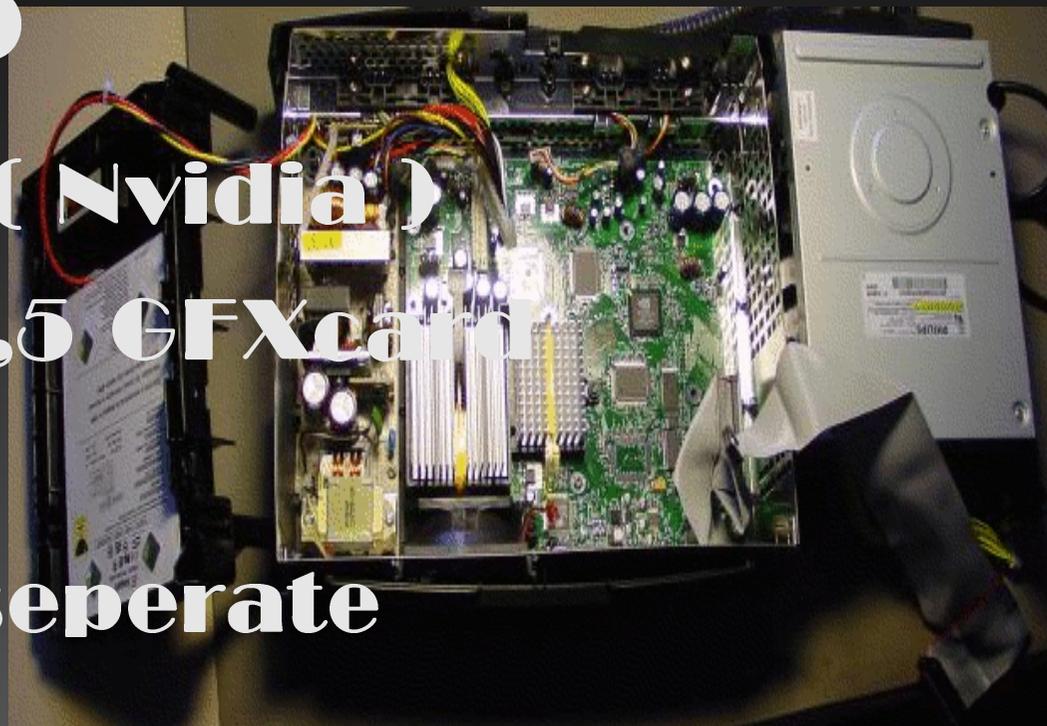
733 Mhz Intel Celeron CPU (based on a PIII)
64 MB RAM

10/100MBit NIC (Nvidia)

Nvidia GeForce 3.5 GFx card

10 GB hardisk

4 USB ports (2 seperate bridges)
DVD Rom drive





Hardware modification

How can I run unsigned code on the Xbox ?

Exchanging the BIOS by :

- Using a modchip
- Replacing the original one

Exploiting a bug in the original dashboard :

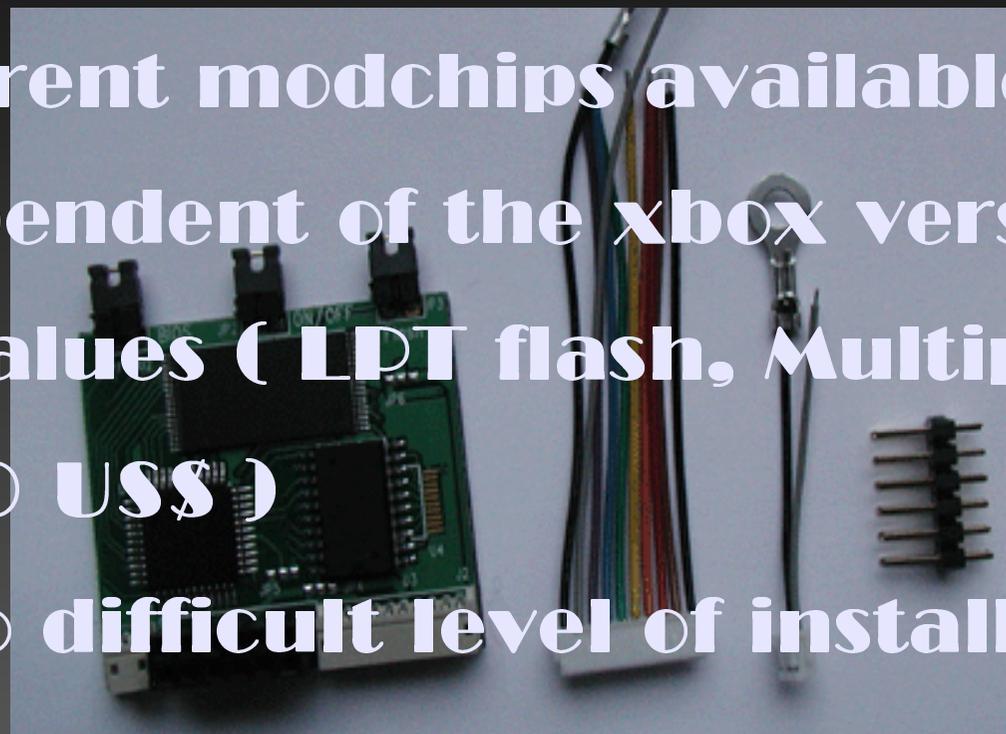
- Font dashboard Hack *
- Audio dashboard Hack

* Recently Microsoft released a patch to this bug / feature

Using a modchip

Bypassing the original bios chip with an modchip

- +/- A lot of different modchips available**
- + Nearly independent of the xbox version**
- + Additional values (LPT flash, Multiple BIOS)**
- Cost (32 - 80 US\$)**
- Medium upto difficult level of installation**





Replacing the original bios

Flashing the original eeprom with a new bios

Therefore we need to enable the "write enable" of the eeprom by installing a switch

Using a known bug to boot into linux to be able to (over)write the eeprom



Xbox models

Currently 6 different models exists :

Version	Eeprom		Cromwell Support	Fabrication Date
	1mb	256kb		
1.0	*		*	< Sep 2002
1.1	*		*	< Dez 2002
1.2		*		< Mar 2002
1.3		*		< July 2003
1.4		*		> July 2003
1.5		*		> Aug 2003

Xbox meets linux



Xbox models (2)



Using the spare memory of the eeprom

(TSOP hack)

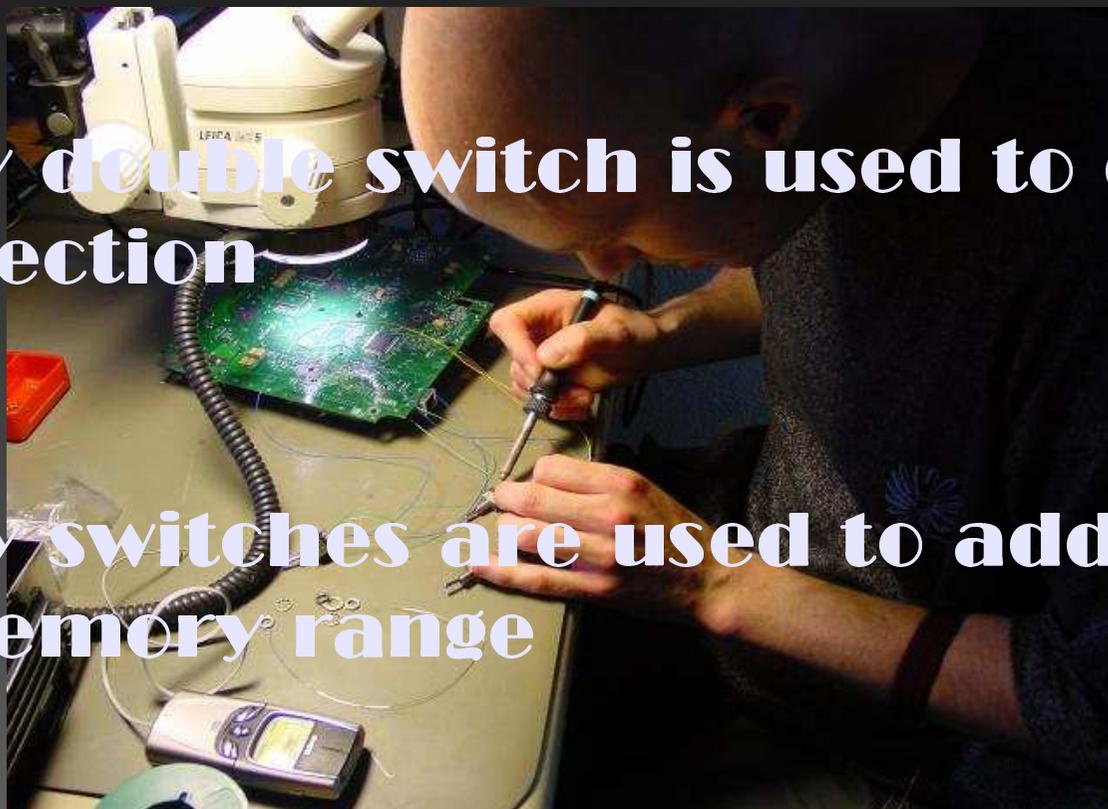
We need to solder 3 additional switches :



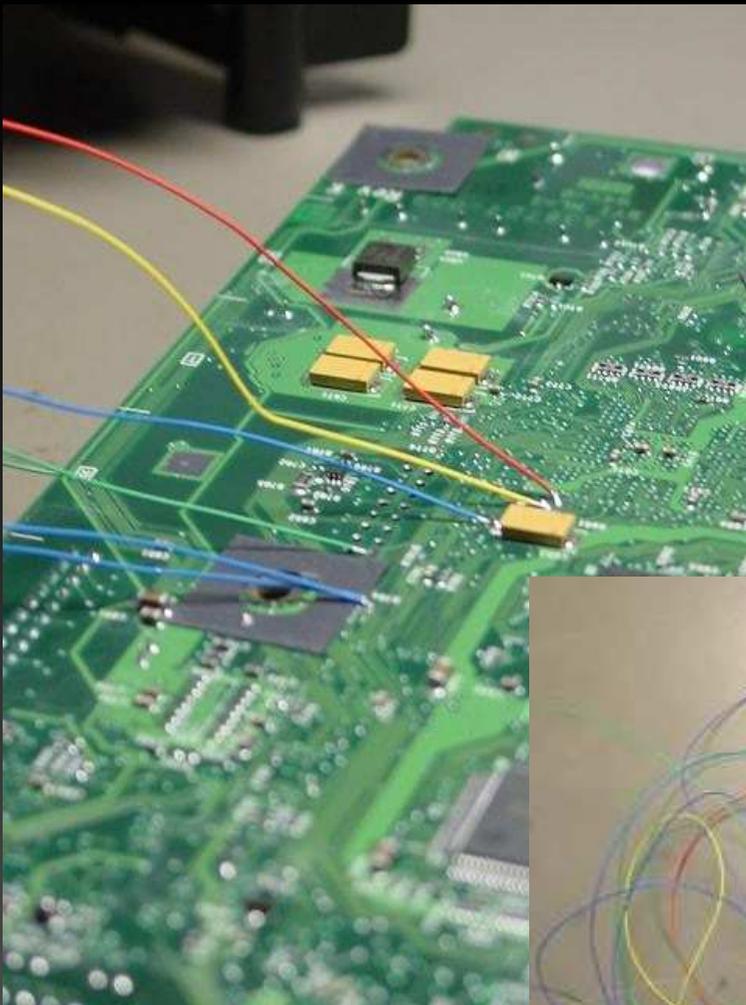
One 2 way double switch is used to disable write protection



Two 3-way switches are used to address the full memory range

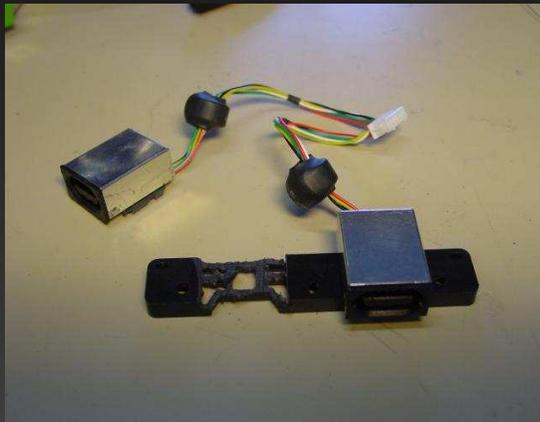


Xbox meets linux



Additional Hardware modifications

USB



Exchange the Harddisk

[Http://510071924555.bei.t-online.de/xsecrets/](http://510071924555.bei.t-online.de/xsecrets/)

Flashing the eeprom with the 007 hack

We need a running linux to be able to flash the eeprom therefore we need :

A copy of the game 007 Agent under Fire

The corresponding savegame hack





Copying the savegame to the Xbox HD

The harddisk can only be unlocked by the original BIOS

1) Compile and boot a linux kernel with the fat filesystem

2) Start the Xbox

3) After the bios unlocked the hd replace the original BIOS

IDE - HOTSWAPING!

4) Mount and copy the savegame

Xbox meets linux





Flashing the eeprom with raincoat

Raincoat is the tool to (over)write the bios

Currently there is one Linux bios but 3 diff. vers

Cromwell : the open-source bios

Xromwell : the xbe version of cromwell

Stardust : modified cromwell for gentoox

Flashing the eeprom with raincoat (2)

```
Eterm
Xbox: raincoat # ls
800x600.bin bios.bin cromwell.bin cromwellv1_22.bin evox.bin raincoat raincoat.conf
Xbox: raincoat # raincoat
Raincoat v0.5 Gentoox Edition - http://gentoox.shallax.com - v1.2 support
Reading /etc/raincoat.conf... 11 flash types read

DETECTED: ST - M29F080A (1024K)

raincoat [-p filetoprog] [-r filetodumpto] [-a hexoffset] [-v]

-p filetoprog      Program flash with given file
-r filetodumpto   Read whole flash back into file
-a hexoffset      Optional start offset in flash, default 0
-v                Verbose informational messages

Example: raincoat -p cromwell.bin

Please note, -p will reprogram your BIOS flash
Please do not use if you don't understand what that
means, there is no simple undo for this if you
programmed the wrong thing.
-r is always safe to use, as is running with no args
Xbox: raincoat # raincoat -a 80000 -p evox.bin
Raincoat v0.5 Gentoox Edition - http://gentoox.shallax.com - v1.2 support
Reading /etc/raincoat.conf... 11 flash types read

DETECTED: ST - M29F080A (1024K)
Programming with evox.bin...Read 262144 bytes from file
Erasing...
Done
Programming...
Done
Verifying...
Done
Completed
Xbox: raincoat # █
```



Installing linux

Currently there are about 4 different linux distros available for the Xbox

Gentoox

[Http://gentoox.shallax.com/](http://gentoox.shallax.com/)

Ed's Xbox Debian GNU/Linux

[Http://xbox-linux.sourceforge.net/debian/](http://xbox-linux.sourceforge.net/debian/)

Dyne:bolic

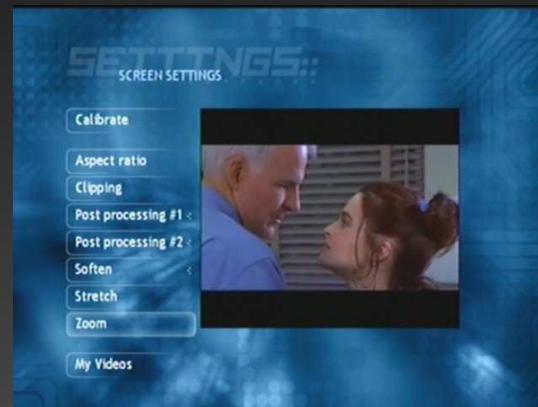
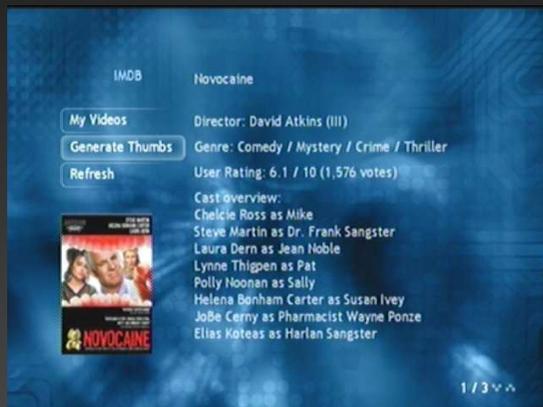
[Http://dynebolic.org/](http://dynebolic.org/)

Slothbox - Slackware for the Xbox

[Http://slothbox.atxconsulting.com/](http://slothbox.atxconsulting.com/)

Practical use

Multimedia station (movies,
music) need linux -> XBMP



Emulator station (Amiga, NES, ...)
Webserver



More links

All information about Xbox hack, a lot of tutor

[Http://www.xbox-scene.com](http://www.xbox-scene.com)

The home of the linux Xbox project

[Http://xbox-linux.sourceforge.net](http://xbox-linux.sourceforge.net)

A very good german tutorial about the TSOP ha

[Http://www.lugal.de](http://www.lugal.de)

Xbox meets linux

