Xbox Hacking

für BWL-Studenten :-)

Michael Steil <mist@c64.org>
Xbox Linux Project
09.05.2005

www.xbox-linux.org

Marketing

Das Xbox Videospielsystem von Microsoft ist das Videospielsystem der Zukunft. Mit Xbox erleben Sie Spiele in bisher unerreichter Qualität. Mit technischen Innovationen wie einer 8-Gigabyte-Festplatte, einem Ethernet-Port sowie einer Rechenleistung von 1.600 Milliarden Operationen pro Sekunde, ermöglicht Xbox den Spieleentwicklern, ihre kreativen Visionen ohne Beschränkungen zu verwirklichen. So entsteht Software, die die Grenzen zwischen Fantasie und Realität verschwinden lässt.

Quelle: Pressemitteilung Microsoft Deutschland, 2002

Technik

- **Intel** Pentium III Celeron, 733 MHz
- **Samsung** 64 MB RAM
- **nVidia** GeForce 4MX
- **Toshiba** 10x DVD-ROM
- **Western Digital** 8 GB Festplatte
- Fast Ethernet (Netzwerk/DSL)
- 4 USB-Anschlüsse


XBOX
XBOX

ALDI informiert

...ab Donnerstag, 28. April

Mobiles Navigationssystem & Pocket-PC in einem!

- GPS-Antenne integriert
- für Auto, Motorrad, Fahrrad und Fußgänger

Funktionen

- **Komplettsystem zur Navigation, Kontakte-/Termin-Verwaltung und Unterhaltung**
- **Sprachausgabe,** farbige Karten- und Pfeilnavigation
- satellitengestützte Positionsbestimmung (GPS)

Technische Daten

- Betriebssystem Microsoft Windows Mobile™ 2003 Software für Pocket PC
- Arbeitsspeicher 64 MB
- Intel® PXA-255 300 MHz Prozessor
- TFT-Display mit 65.536 Farben
- **SD/MMC-Steckplatz**
- **Gewicht ca.:** 147 g
- **Maße ca.:** 11,2 x 7 x 1,6/2,4 cm

Weiteres im Lieferumfang, z.B.:
Docking Station, Autohalterung , Fahrradhalterung, 12 Volt Auto-Ladekabel…

320MB
64MB* on board
plus 256MB
MMC Speicherkarte

* 28 MB bereits vom Betriebssystem genutzt.

Auspacken Einschalten Navigieren

3 Jahre Garantie Mit Service-Hotline.

359,–*

Kartenmaterial für komplett Westeuropa (inkl. Haupt- und Nebenstraßen) im Lieferumfang
(Deutschlandkarte vorinstalliert).

MEDION MD 95000 mit Windows Mobile™ Software – umfangreiches Software-Paket!

Designed for Windows Mobile™

MEDION

Tele Atlas SiRF

4 in 1 Digitale Slimline Kamera

1. Mobile digitale Kamera
2. Digitaler Camcorder
3. PC-Kamera
4. Voice Recorder

- **3,0 Megapixel**
- **4 x Digital-Zoom**
- **SD-/MMC-Kartenslot zur Speichererweiterung**
- **1,5" Farb-LCD-Bildschirm**

USB UNIVERSAL SERIAL BUS

Inkl. Zubehör.

3 Jahre Garantie

69,99*

Digitaler Twin SAT-Receiver

Mit 80 GB Festplatte!

TEVION

- **Twin Tuner für gleichzeitiges Aufnehmen und Anzeigen von zwei versch. Programmen**
- **Time Shift Funktion für zeitversetztes Fernsehen**
- **Electronic Program Guide**
- **6.000 Programm-Speicherplätze**
- **800 Seiten Super Fast Videotext**
- 2 Scart-Anschlüsse
- mehrsprachiges OSD Menü

Maße ca.: 32 x 6 x 25 cm (B x H x T)

Auch in Anthrazit.

3 Jahre Garantie

je 249,–*

*Bitte beachten Sie, dass diese Aktionsartikel im Unterschied zu unserem ständig vorhandenen Sortiment nur in begrenzter Anzahl zur Verfügung stehen. Sollten bestimmte Produkte, trotz unserer sorgfältigen Planung, aufgrund unerwartet hoher Nachfrage u. U. schon am ersten Aktionstag ausverkauft sein, bitten wir um Ihr Verständnis.

WELTNEUHEIT TV für ALLE!	**DVB-S** Digitaler Satellitenempfang[1] **DVB-T** Das digitale Überall-TV[1+3] **ANALOG-TV** eingebaute Tunerkarte mit analog Stereo-TV & FM Radio-Tuner
Arbeitsspeicher	**1.024 MB** RAM DDR 400 MHz 64 Bit dual channel memory (1 Bank frei zur Aufrüstung)
ATI	**ATI Radeon X740 XL** Grafikkarte mit TV-Out Anschlüssen über Scart, S-Video oder Composite. Superschneller GDDR3 Speicher mit 900MHz. ATI X740 XL Grafikprozessor mit 425 MHz. PCI-Express x16 Bus-Konzept.
WESTERN DIGITAL	**300 GB** Festplattenkapazität 8 MB Cache Superschnelle 7200 U/Min. S-ATA 150 Interface MEGA-LEISTUNG!
MEDION	**WLAN** 54 Mbit/s IEEE 802.11g 802.11b kompatibel Drahtloser Netzwerkzugang[2], der perfekte Einstieg in die kabellose Netzwerktechnologie zu Hause, im Büro... [2] Vorausgesetzt am Standort befindet sich ein WLAN Access Point.
PIONEER	**16x Dual Layer, Multi-Standard DVD-/CD-Brenner[4]**
LG	**16x DVD-ROM**
DOLBY DIGITAL	**8 Kanal Intel® High Definition Audio** (Nur in Verbindung mit geeigneten Lautsprechersystemen/nicht im Lieferumfang enthalten.)
MEDION	**Bluetooth** Funkstandard
FIREWIRE	**2x Firewire** (IEEE 1394) 1x Front, 1x Rückseite
USB 2.0	**6x USB 2.0** 2x Front, 4x Rückseite
DSL & Network Ready	Netzwerkcontroller on board Fast Ethernet 10/100 Mbit/s
MEDION	56K V.9x PCI Daten Fax Modem

[1] Entsprechende Antenne erforderlich, nicht im Lieferumfang enthalten.
[2] Vorausgesetzt am jeweiligen Standort werden DVB-T bzw. digitale Dienste angeboten.

[4] Sie dürfen nur Kopien des Materials erstellen, dessen Urheberrechtsinhaber Sie sind bzw. für das Sie vom Urheberrechtsinhaber eine Kopiererlaubnis erhalten haben. Wenn Sie nicht der Urheberrechtsinhaber sind bzw. keine Kopiererlaubnis vom Urheberrechtsinhaber erhalten haben, verletzen Sie möglicherweise das Urheberrecht und unterliegen eventuell Schadensersatzansprüchen.

Intel, Intel Logo, Intel Inside, Intel Inside Logo, Intel Centrino, Intel Centrino Logo und Pentium sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

MEDION PC TITANIUM MD 8386 XL

...AULTIMEDIA HOME
EN... ...T DESIGN CENTER

Nach Ein... ...scheins e... ...n Sie zusätzlic... ...Zub...

- 256 MB Mem...
- Webcam
- PC-Lautsprecher
- Scart-Kabel

Den Gutschein erhalten Sie beim Kauf dieses PCs an der Kasse!

- zukunftssichere Technologie durch 64 bit Unterstützung
- 2 MB Cache, verdoppelter L2 Cache für optimale Performance
- geräuscharm durch AIRXL Heat Pipe Ki...er und SpeedStep® Technologie

Inkl. umfangreichem Software-Paket!

Computer-Bild Ausgabe 6/2005
Platz 1
in der COMPUTER-BILD-Bestenliste
Note 1,53

Computer-... Ausgabe 6/200...
Bestes Ge... in der Bestenlist...

Testergebnis	gut
Preis-Leistungs-Verhältnis	sehr gut

"Fazit: Aldi schnürt wieder mal ein tolles Paket aus schnellem Computer, viel Software und sehr umfangreicher Ausstattung. Ein Top-PC zum Schnäppchenpreis."

Intel® Pentium® 4 Prozessor 640 mit HT-Technologie
3.2 GHz, 2MB L2 Cache, 800 MHz FSB

intel inside pentium 4

WELTNEUHEIT
Die ...ere Serie
...neueste Intel® Prozessorarchite...r!

...t Service-Hotline.
... Jahre Garantie

949,–*

ALDI SÜD

19" Aktiv SXGA LCD-Flachbildschirm

Inkl. Zubehör.

299,–*

- **sichtbare Bildschirmdiagonale:** 48,2 cm
- **Reaktionszeit typ.:** 8 ms
- **Kontrastverhältnis typ:** 700:1
- **Helligkeit typ.:** 300 cd/m²
- **Betrachtungswinkel typ.:** horizontal 150°, vertikal 135°
- **VGA/DVI-D-Anschluss**
- **max. Auflösung: 1.280 x 1.024**
- On Screen Display
- 2 integrierte Lautsprecher

3 Jahre Garantie

TCO Development TCO'03 DISPLAYS www.tcodevelopment.com

Weitere Informationen zu den Aktionsartikeln finden Sie unter:
www.aldi-sued.de · wap.aldi.de

17T-3-2005

ALDI informiert +++ ALDI informiert +++ ALDI informiert +++ ALDI informiert

Inhalt

- Entstehungsgeschichte der Xbox
- Xbox-Hacker
- Open Source & Linux
- Xbox-Hacks (Sicherheitssystem)
- Xbox-Linux
- Praxis

ca. 1985

IBM PC
s/w Textbildschirm

Markt 2005
95%

Baugleiche drücken Preis

Apple Macintosh
s/w Grafikbildschirm

Markt 2005
5%

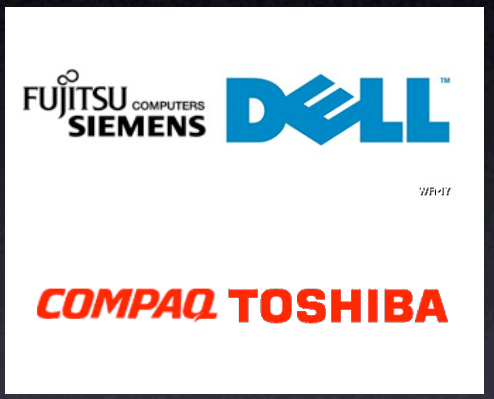
Commodore Amiga
farbiger Grafikbildschirm

† 1995

Microsoft

- ...ist der Gewinner
- MS-DOS auf allen PC-kompatiblen
- Nachfolger: Windows
- zu Windows passende Software:

  Word, Excel, Powerpoint, Access, ...



Microsoft 2000

- Microsoft ist Monopolist bei
  - Betriebssystemen (Windows)
  - Bürosoftware (Word, Excel)
- Neuer Markt Unterhaltungsmedien

→ Ausweitung des Monopols auf der Wohnzimmer

Das Wohnzimmer

SONY	Microsoft®
Discman, Mini-Disc	Windows Media Audio
DVD Recorder	Windows Media
Playstation	

Wir bauen eine Spielekonsole

und zwar möglichst schnell!

- Man nehme:
  - einen PC
  - ein schickes Gehäuse
- fertig!

Seamus Blackley

(nun darf uns nur keiner draufkommen, daß wir eigentlich nur einen umverpackten PC verkaufen)

Ein wenig Technik...

- Prozessor von Intel
- Grafik von nVidia
- Windows als Betriebssystem
  (ohne Fenster, Maus)
- eingebauter Kopierschutz

...und Schutz, Xbox als PC zu verwenden...

Hardware subventioniert; Geld wird mit Spielen verdient

Hacker

- nicht verwechseln mit Cracker!
  - = Raubkopien in Umlauf bringen
  - = Firmennetze zur eigenen Bereicherung angreifen
- sondern:
  - spielerischer Umgang mit Technik
  - Herauskitzeln von Möglichkeiten

Beispiele

Blinkenlights
Hochhaus als Bildschirm

Sony AIBO
mit gehackter Software
kann er Jazzdance

Nokia dbox2
mit gehackter Software:
Tetris-Spielen in den Werbepausen

Hacker

SANDRA BULLOCK
THE NET

Die Simpsons


THE MATRIX
Fotos.org

KEANU REEVES LAURENCE FISHBURNE
MATRIX


MICROSOFT

Die Xbox ist ein PC

- Wieso also nicht als PC nutzen?
- die Xbox ist
  - klein
  - billig (149 EUR)

also ideal für...

- Musik und Video im Wohnzimmer
- Internet & Email im Wohnzimmer
- kleiner Arbeitscomputer
  (Textverarbeitung usw.)
- Server (MP3- und Video-Speicher)

weitere Motivation

- Hacken macht Spaß
- Microsoft ärgern macht Spaß
- Ich kaufe einen PC und “darf” nur spielen??

Welches Betriebssystem?

- Die Xbox ist nicht 100% PC-kompatibel
- Das Betriebssystem muß leicht angepaßt werden

Microsoft, könnt Ihr bitte Windows so anpassen, daß es auf der Xbox läuft?

(wohl kaum)

```
1527 /*
1528  * Initially all pages are reserved - free ones are freed
1529  * up by free_all_bootmem() once the early boot process is
1530  * done. Non-atomic initialization, single-pass.
1531  */
1532 void __init memmap_init_zone(unsigned long size, int nid, unsigned long zone,
1533                 unsigned long start_pfn)
1534 {
1535         struct page *start = pfn_to_page(start_pfn);
1536         struct page *page;
1537
1538         for (page = start; page < (start + size); page++) {
1539                 set_page_zone(page, NODEZONE(nid, zone));
1540                 set_page_count(page, 0);
1541                 reset_page_mapcount(page);
1542                 SetPageReserved(page);
1543                 INIT_LIST_HEAD(&page->lru);
1544 #ifdef WANT_PAGE_VIRTUAL
1545                 /* The shift won't overflow bec
1546                 if (!is_highmem_idx(zone))
1547                         set_page_address(page,
1548 #endif
1549                 start_pfn++;
1550         }
1551 }
```

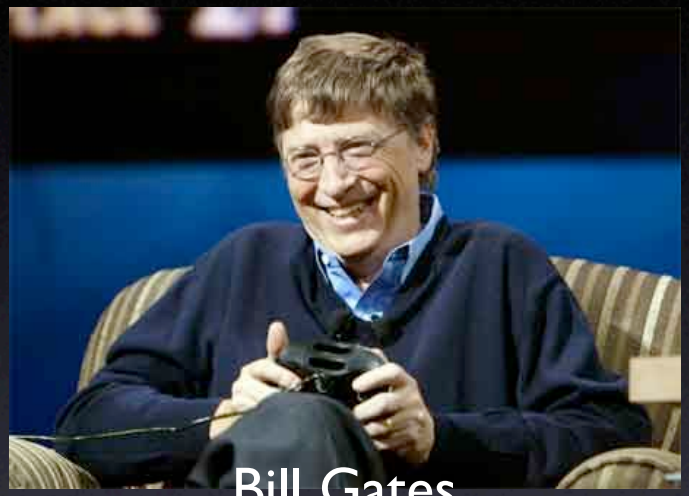
Source Code (Entwicklung)

Binary Code (Auslieferung)

```
00000000  00 00 15 4f 6d 6f 6f 76  00 00 00 6c 6d 76 68 64
00000010  00 00 00 00 be 2d 5d df  be 2d 5d df 00 00 00 0a
00000020  00 00 04 81 00 01 00 00  01 00 00 00 00 00 00 00
00000030  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00
*
00000050  00 00 00 00 40 00 00 00  00 00 00 00 00 00 00 00
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000070  00 00 00 02 00 00 00 18  69 6f 64 73 00 00 00 00
00000080  10 80 80 80 07 ff 8f ff  ff 00 01 ff 00 00 14 c3
00000090  74 72 61 6b 00 00 00 5c  74 6b 68 64 00 00 00 01
000000a0  bd 08 e2 6e bb f4 a6 1c  00 00 00 01 00 00 00 00
000000b0  00 00 04 81 00 00 00 00  00 00 00 00 00 00 00 00
000000c0  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00
*
000000e0  00 00 00 00 40 00 00 00  01 40 00 00 00 f0 00 00
000000f0  00 00 14 5f 6d 64 69 61  00 00 00 20 6d 64 68 64
00000100  00 00 00 00 bd 08 e2 6e  bb f4 a6 1c 00 00 00 0a
00000110  00 00 04 81 00 00 00 00  00 00 00 21 68 64 6c 72
00000120  00 00 00 00 00 00 00 00  76 69 64 65 00 00 00 00
00000130  00 00 00 00 00 00 00 00  00 00 00 14 16 6d 69 6e
00000140  66 00 00 00 14 76 6d 68  64 00 00 00 01 00 00 00
00000150  00 00 00 00 00 00 00 00  24 64 69 6e 66 00 00 00
00000160  1c 64 72 65 66 00 00 00  00 00 00 00 01 00 00 00
```

Open Source

- Closed Source:
  - Quelltext ist Betriebsgeheimnis
  - Softwarehersteller hat die vollständige Macht über sein Produkt
- Open Source:
  - Quelltext ist frei (und kostenlos) verfügbar
  - Jeder kann das Programm erweitern und verbessern
  - Geld wird indirekt verdient



Bill Gates
Microsoft Corporation

Richard Stallman
Free Software Foundation

Open Source

- herstellerunabhängig
- höhere Qualität (mehr Augen)
- kostenlos für den Anwender

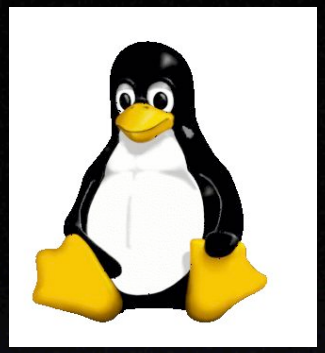
Open Source

Firefox

OpenOffice.org

Thunderbird

Linux



Linux

- Open Source Betriebssystem
- kostenlos
- unabhängig von Herstellern
- keine Viren, keine Abstürze
- benutzerfreundlich
- alle nötige Software bereits dabei

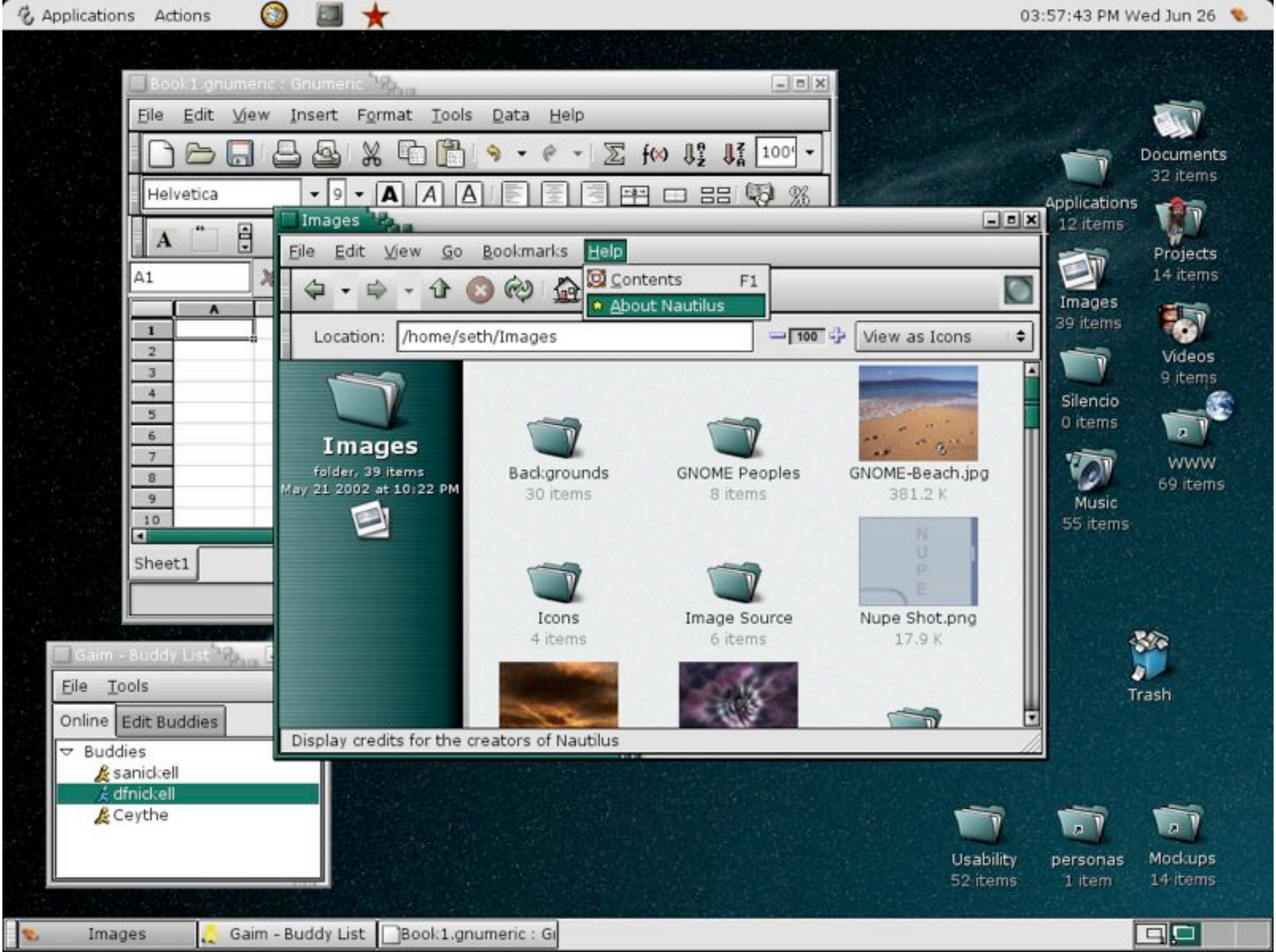
suse
A NOVELL COMPANY

redhat

debian

ubuntu

Linux Mandrake

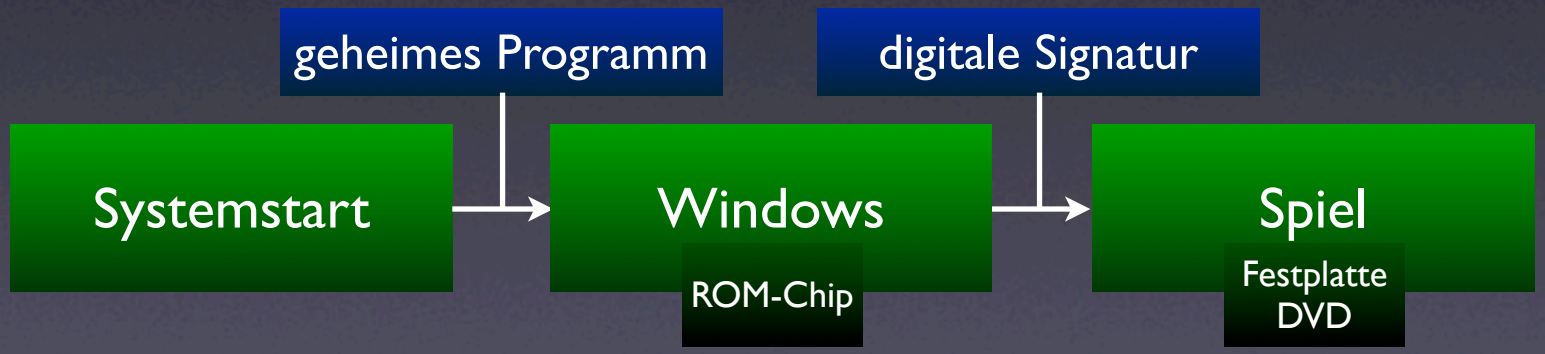

Applications
Actions
03:57:43 PM Wed Jun 26
Book1.gnumeric : Gnumeric
File Edit View Insert Format Tools Data Help
Helvetica
A1
Sheet1
Images
File Edit View Go Bookmarks Help
Contents F1
About Nautilus
Location: /home/seth/Images
100
View as Icons
Images
folder, 39 items
May 21 2002 at 10:22 PM
Backgrounds
30 items
GNOME Peoples
8 items
GNOME-Beach.jpg
381.2 K
Icons
4 items
Image Source
6 items
Nupe Shot.png
17.9 K
Display credits for the creators of Nautilus
Gaim - Buddy List
File Tools
Online
Edit Buddies
Buddies
sanickell
dfnickell
Ceythe
Documents
32 items
Applications
12 items
Projects
14 items
Images
39 items
Videos
9 items
Silencio
0 items
WWW
69 items
Music
55 items
Trash
Usability
52 items
personas
1 item
Mockups
14 items
Images
Gaim - Buddy List
Book1.gnumeric : Gi

Xbox-Linux

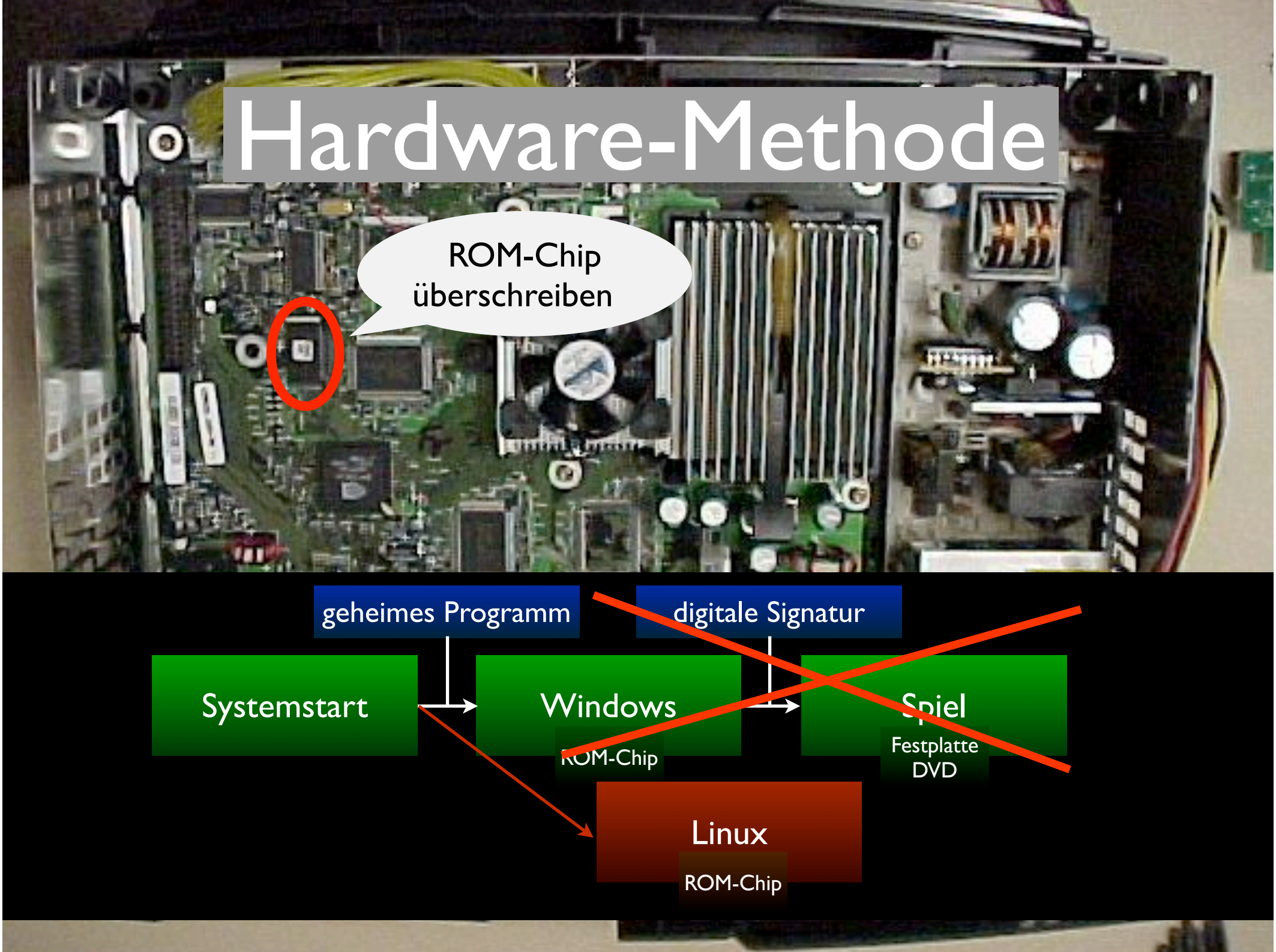
- Sicherheitssystem umgehen
- Dual-Boot
- Bootloader
- Linux anpassen
- Wohnzimmeroptimierung

Sicherheitssystem

- Idee: es darf niemals Programmcode laufen, der nicht berechtigt ist
- Chain-Of-Trust



Hardware-Methode

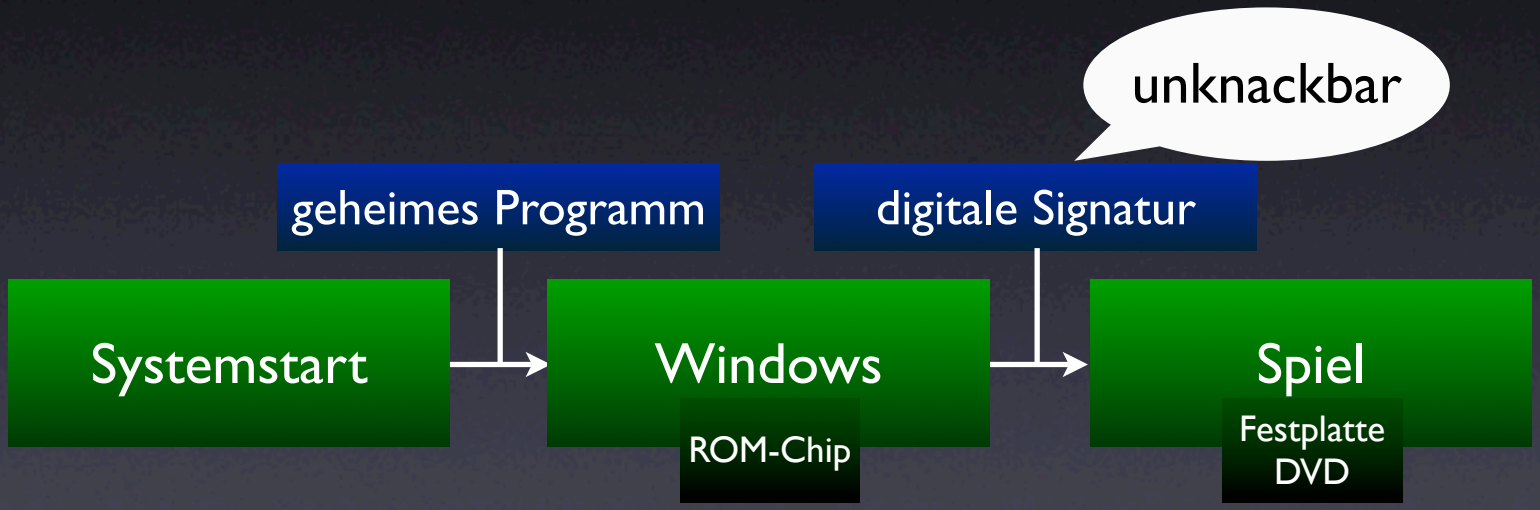


Hardware-Methode

- Windows wird komplett ersetzt
- Spiele nicht mehr möglich
- Löten notwendig
- aber volle Flexibilität
  - Festplatte ersetzen
  - DVD-Laufwerk ersetzen

    (z.B. durch Brenner)

Software-Methode



was nun??

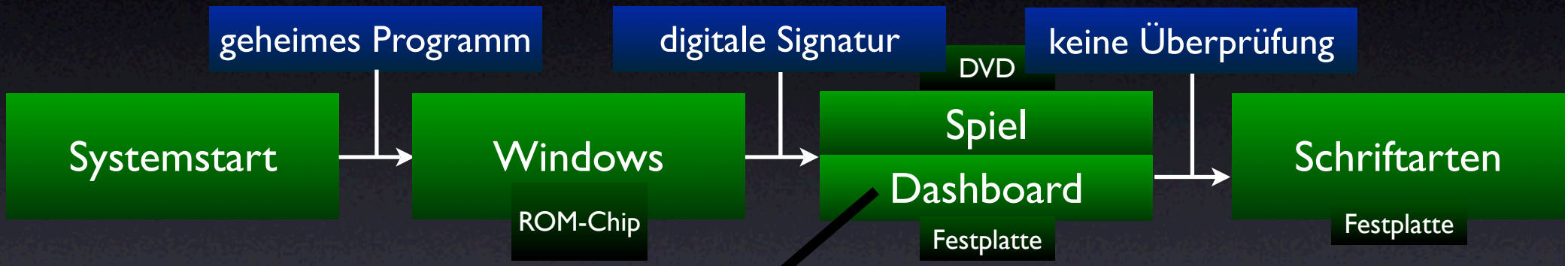
Software-Methode

Software-Methode

- gehackten Spielstand auf Memory Card laden
- 007 starten
- Spielstand einlesen
- Linux startet

brauch ich das Spiel jedes Mal???

Software-Methode



Menüsystem, wenn kein Spiel eingelegt ist

vollständige Prozedur

- gehackten Spielstand auf Memory Card laden
- in 007 Spielstand auswählen
- der Hack kopiert gehackte Schriftarten auf die Festplatte
- bei jedem Einschalten ohne Spiel wird der Hack auf Festplatte aktiv!


MEMORY
MUSIC
LINUX
SETTINGS
A
SELECT

Software-Methode

- Windows bleibt drauf
- Spiele weiterhin möglich
- kein Öffnen der Xbox notwendig
- aber eingeschränkte Flexibilität
  - Teile der Festplatte belegt
  - DVD-Laufwerk muß bleiben

Xbox Linux

- Läuft nach Hardware- oder Software-Modifikation
- mit Fernbedienung bedienbar
- beinhaltet
  - Media Player (DivX, MP3)
  - Webbrowser, E-Mail

Praxis

- man braucht:
  - eine Xbox (je älter, desto besser)
  - einen USB-Stick (einmalig)
  - einen USB-Adapter (einmalig)
  - eins der Spiele (einmalig)
  - Xbox-Linux CD (aus dem Internet)

Users Help Users

Stéphan Schamp (*5)	Hobbyist	Oost-Vlaanderen Wichelen Serskamp 9260 **Belgium**	stephanschamp@hotmail.com	Y	Y	Y	Y	N	N	usb cable or xbox cable (to solder t I dont know about female or male. I
Damien Littré	Hobbyist	1780 Wemmel **Belgium**	xboxlinux@littre.be	Y	N(*1)	Y	Y	N	Y	http://www.littre.be/page.php?page=
Giancarlo Conetta	Hobbyist	Aurora, Ontario, L4G 6E5 **Canada**	A_____Z@msn.com Phone: 905 841 2804	Y	Y	Y	Y	Y	Y	A visit from the person is a cool gif to, then anything that u think id like it; I can also help you by phone
Jérôme Nicolle	Hobbyist	27200 Vernon, **France**	xboxlinux@free.fr	Y	Y (*8)	Y	Y	Y	Y	Anything, mostly xbox related, at le nice gift could be a blowjob offer ;)
Michael Steil	Xbox-Linux team member	D-80797 München **Germany**	steil@in.tum.de	Y	Y	Y	Y	Y	Y	non PC-Hardware (PowerPC,HP-PA
Rüdiger Biernat	HOWTO Translator	D-44787 Bochum **Germany**	info@24prompt.de	Y	Y	N	N	Y	Y	Any bar of chocolate OR Lucky Str Bull OR for the rich ones: Some old Sun-machines
Thomas Wuensche	Hobbyist	85304 Ilmmuenster **Germany**	wuensche@ems-wuensche.com	N	Y	Y	Y	Y	N	-
		D-85435 Erding							

Die Xbox im Wohnzimmer...


debian
xbox

oder gleich gscheit...

(Hotel Royal, Schillerstraße)


XBOX
XBOX
XBOX


SEEMOLLER

Fazit

- Die Xbox ist ein PC
- Microsoft ist böse
- Hacker sind die Guten
- Open Source ist toll
- Linux auf der Xbox ist
  - einfach hinzukriegen
  - sinnvoll