NDS - Fakten und Anderes

Nintendo DS

duracell, Marcel_, mm, TobiX

Chaos Computer Club Cologne e.V.
http://koeln.ccc.de

27.07.2006 Vortrag

Gliederung

Gliederung

Der CCC

Aktionen

TUWAT, 1KT Version

Daß die innere Sicherheit erst durch Kompu-tereinsatz möglich wird, glauben die Mächtigen heute alle. Daß Komputer nicht streiken, setzt sich als Erkenntnis langsam auch bei mittleren Unternehmen durch. Daß durch Komputereinsatz das Telefon noch schöner wird, glaubt die Post heute mit ihrem Bildschirmtextsystem in „Feldversuchen" beweisen zu müssen. Daß der „personal computer" nun in Deutschland dem videogesättigten BMW-Fahrer angedreht werden soll, wird durch die nun einsetzenden Anzeigenkampag-nen klar. Daß sich mit Kleinkomputern trotzalledem sinn[illegible]e Sachen machen las-sen, die keine zentralisierten Großorganisa-tionen erfordern, glauben wir. Damit wir als Komputerfrieks nicht länger unkoordi-niert vor uns hinwursteln, tun wir wat und treffen uns am 12.9. 81 in Berlin, Wattstr. (TAZ-Hauptgebäude) ab 11.00 Uhr. Wir reden über: internationale Netzwerke - Kommunikationsrecht - Datenrecht (Wem gehören meine Daten?) - Copyright - Informations- u. Lernsysteme - Daten-banken - Encryption - Komputerspiele - Programmiersprachen - processcontrol - Hardware - und was auch immer.

Tom Twiddlebit, Wau Wolf Ungenannt (» 2)

Damit fing es an
'Die Tageszeitung'
1.9.81

Vereinsziele

- Einsatz für ein Menschenrecht auf zumindest weltweite ungehinderte Kommunikation
- Förderung von Informationsfreiheit und Transparenz (z.B. maschinenlesbare Regierung)
- Auseinandersetzung mit gesellschaftlichen Folgen von Technologie
- Einsatz für Bürgerrechte und Privatssphäre
- Gesetzes- und Implementationsfehler früh erkennen und in Zusammenarbeit mit Politik, Wirtschaft und Industrie Abhilfe schaffen

→ „Schnittstelle zwischen Technik und Gesellschaft“

Vereinsziele

- Einsatz für ein Menschenrecht auf zumindest weltweite ungehinderte Kommunikation
- Förderung von Informationsfreiheit und Transparenz (z.B. maschinenlesbare Regierung)
- Auseinandersetzung mit gesellschaftlichen Folgen von Technologie
- Einsatz für Bürgerrechte und Privatssphäre
- Gesetzes- und Implementationsfehler früh erkennen und in Zusammenarbeit mit Politik, Wirtschaft und Industrie Abhilfe schaffen

→ „Schnittstelle zwischen Technik und Gesellschaft“

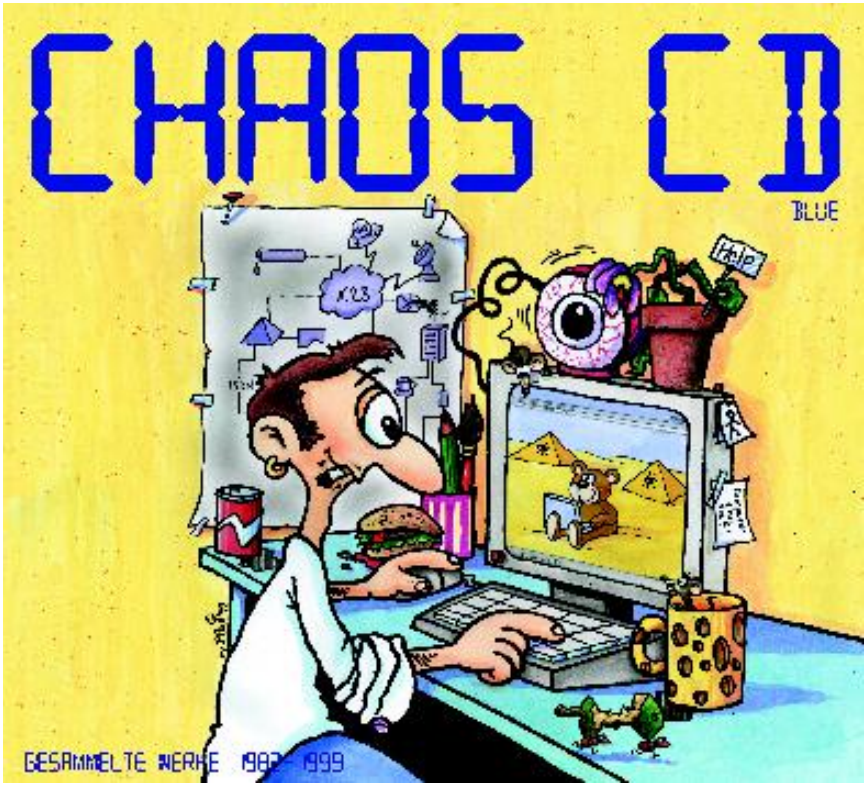
Praktische Arbyte / Organisationsform

Intergalaktische Gemeinschaft, organisiert in Dezentralen, Erfa-Kreisen und Chaostreffs

1500 Mitglieder, 13 Erfa-Kreise, etliche Chaostreffs, „Chaos Family“

Praktische Arbyte / Organisationsform

Betrieb von Kommunikationsstrukturen und Medien



Chaos CD, Die Datenschleuder

Gliederung

Einleitung

„DS Sells 20 million, 17 Million More by March 2007“ (slashdot.org)

Hardware

- 2 TFT Farb LCD Bildschirme mit 256x192 Pixel Auflösung, der untere als Touchscreen
- Haupt-CPU: ARM946E-S (67 MHz)
- Hilfs-CPU: ARM7TDMI (33 MHz)
- W-LAN 802.11b und Nintendos eigenes „NiFi“ Protokoll
- Eingebautes Mikrofon, A/B/X/Y/L/R Buttons, Start, Select, Controlpad
- 4MB Hauptspeicher
- GBA Slot, NDS Slot
- bis zu 10 Stunden Akkulaufzeit

Gliederung

Original Firmware

- Kann vom NDS-Slot nur Blowfish-verschlüsselten Code laden.
- Nimmt nur RSA-signierte WiFi-Download-Games an
- Verschwendet allerdings recht viel Platz, ist nicht so gross wie der Flashspeicher
- Kann nur mit DS Code geflasht werden.
- Besteht aus zwei Teilen, Level 1 kann nur durch kurzschliessen eines Kontaktes geflasht werden.

FlashMe

FlashMe wurde von „Loopy, FireFly und DarkFader“ entwickelt und ermöglicht es, vom GBA-Slot direkt NDS-Code auszuführen.

- Homebrew Software
- „Pirated“ Roms
- Wifi Spiele funktionieren
- 1. + 2. Level Firmware
- Kein RSA Signature Check mehr bei Download Play
- Kein Health-Warning Screen mehr (optional)

GBA Flash Karte

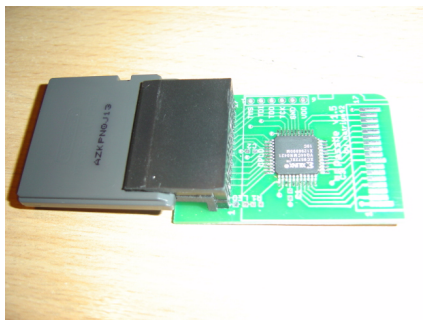
Eine Karte, die in den GBA-Slot eingesteckt wird, üblicherweise Adapter auf SD/CF.

EZ IV Lite / G6 Flash / M3 SD Slim

PassMe

Um DS Code vom GBA-Slot auszufuehren, muss man ein wenig tricksen:

WifiMe	Fehler im WiFi Download Play Code (funktioniert nur mit älterer DS-Firmware)
PassMe	Hardware, benutzt Authentifizierungscode eines Originalspiels
PassMe2	Wird auf spezielles Originalspiel programmiert; notwendig wegen neuer DS Firmware
NoPass	Grösse eines normalen NDS Spiels, genauso verschlüsselt



Passme / Passme2

Gliederung

Linux on every device!

DSLinux wird hauptsächlich entwickelt von Malcolm ‘pepsiman’ Parsons und Stefan ‘stsp’ Sperling.
Vorteile:

- Multitasking
- Stabiler IP-Stack
- Breite Softwareauswahl

Probleme:

- Nur 4MB RAM
- keine MMU

Da der DS keine MMU hat, benutzt DSLinux einen uClinux-Kernel. Ohne MMU gibt es auch keine virtuellen Speicher, also keine getrennten Adressräume oder Unterstützung für Swap.

Kernel

Funktionsfähige Treiber:

- Wi-Fi (DHCP manchmal instabil(?))
- Audio Out (ALSA)
- Framebuffer
- Touchscreen
- Treiber für Massenspeicher in den meisten Flash-Adapter (GBAMP CF, SuperCard CF/SD, M3 CF)

TODO:

- Treiber für Massenspeicher für ein paar Flash Adapter (M3 SD, MagicKey2/3 SD)
- Treiber für DS-Speicherstände
- Audio In

Anwendungen

Läuft schon:

- Diverse Konsolenspiele: bsdgames, frotz, etc.
- SSH via DropBear
- Tiny-X mit VNC-Client (instabil)

Sinnvolle zukünftige Erweiterungen:

- Opie oder andere PDA-Anwendungen
- Handschrifterkennung statt Tastatur?

Gliederung

Gliederung

Emulatoren

Emulatoren für den PC

- Dualis - DS Emulator für Windows, kann nur Demos emulieren und keine NDS Dumps
- iDeaS - DS Emulator für Windows, kann Demos und NDS Dumps emulieren
- DeSmuME - OpenSource DS Emulator, kann Demos und NDS Dumps emulieren, es gibt auch eine Linux Version!
- NO$GBA - Sehr schneller und kleiner GBA/DS-Emulator für DOS/Windows

Emulatoren

Emulatoren für den NDS

- SnezziDS - SNES Emulator für den NDS
- snesDS - SNES Emulator für den NDS
- PocketSPC - SNES Sound Chip Emulator für den NDS
- nesDS - NES Emulator für den NDS
- ScummVM DS - ScummVM Port für den NDS
- CalcEmu - Emuliert den Ti 85 auf dem NDS

Gliederung

WFC

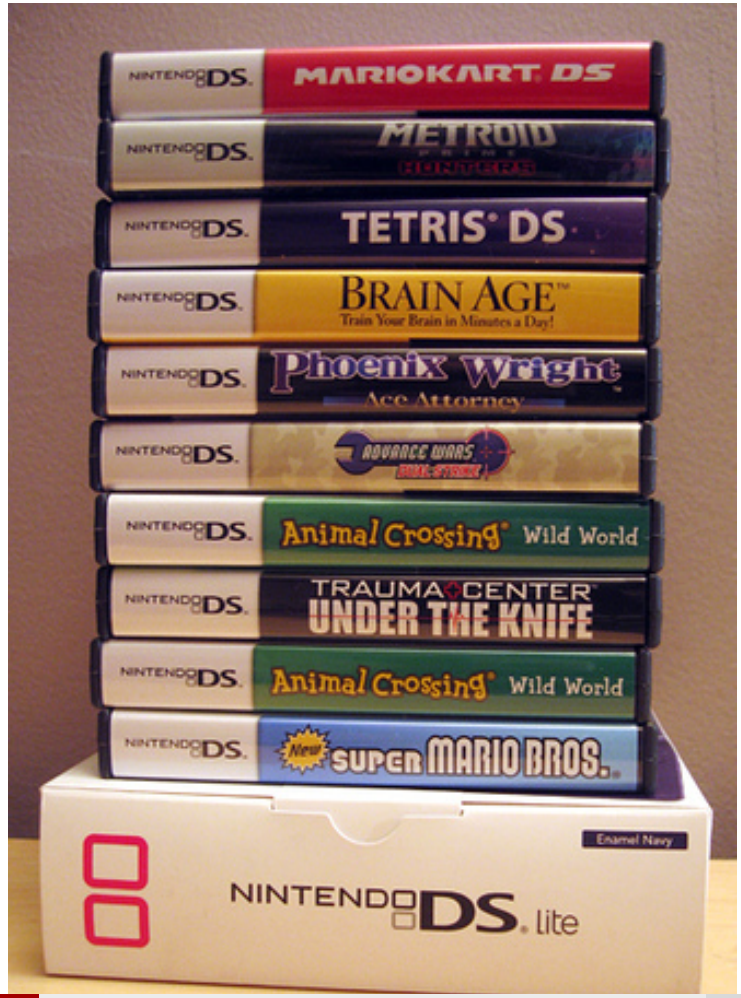
Nintendo Wifi Connection

Multiplayer funktioniert entweder Ad-Hoc oder ueber das Internet mit WFC.

- Teilweise mit Master Servern von Gamespy
- P2P Spiele (Mario Kart)
- Authentifizierung gegenueber WFC mit SSLv3 (+ Server Zertifikat Check)
  NDS ID + Game ID ?
- Nach der Authentifizierung am WFC ist die NDS IP beispielsweise an T-Online Hotspots zum Umstonst-Surfen freigeschaltet. (uiuiuiui)

Games

„Not to mention that there are actual games out for it.“ (slashdot.org)



Gamez

Zur Zeit:

Europe	118 Titel
US	133 Titel
Japan	225 Titel

Ausblick

- Opera Browser mit GBA Slot Speichererweiterung
- Linux mit grafischer Oberfläche?
- Mehr Wifi Homebrew?
- Wlan Scanner mit Capture auf SD Karte?
- ...

Literatur und Links

- http://wiki.pocketheaven.com/
- http://masscat.afraid.org/ninds/wifi_investigation.php
- http://akkit.org/dswifi/
- http://darkfader.net/ds/
- http://devkitpro.org/
- http://www.auia.net/ds/ (NDS Tech Wiki)