Other Wireless

New ways to be Pwned

Luis Miras
luis@ringzero.net
What I’m *Not* Covering
What I Will Be Covering
Attack

• Passive (Sniffing)
  – authentication data
  – sensitive data
• Active (Injection)
  – Denial of Service
  – Execution of arbitrary commands
RF

- RF design is hard, not needed.
- Scanners are not needed.
- Devices come with TX and RX circuits. (use them)
- Think of TX and RX circuits as a network socket.
Let’s get HIDphy!!
HID – human interface device

• Keyboard
  – HID codes similar to ps/2 scan codes

• Mice
  – Relative movements and buttons
  – Positional movement and buttons
Vendor Name: Kensington
Product Name: Wireless Presentation Remote
Serial No:

VID: 047D
PID: 2010
Version: 0100

max Report Length (including Report ID):

Languages

Strings
2) Kensington
3) Wireless Presentation Remote
4) 0008001
5) Wireless USB Device

Collections
- Wireless Presentation Remote
  - Generic Desktop: Keyboard (Application)
Device Research
Wireless Presentation Remote
Serial No. Model #: 33062
F0526077081
Kensington Technology Group
www.kensington.com
FCC ID: GV333062
800-535-4242 Rating: 3V 0.01A
Tested to comply with FCC Standards.
Made in China
FOR HOME OR OFFICE USE.
900-0875-00
### OET Exhibits List

9 Matches found for FCC ID 'GV333062'

<table>
<thead>
<tr>
<th>View Attachment</th>
<th>Exhibit Type</th>
<th>Description of Exhibit</th>
<th>Date Submitted to FCC</th>
<th>Display Type</th>
<th>Date Available</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Block Diagram</td>
<td>BLOCK DIAGRAM</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>External Photos</td>
<td>EXTERNAL PHOTOS</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>ID Label/Location Info</td>
<td>ID LABEL SAMPLE 10/02/2003 AND LOCATION</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Internal Photos</td>
<td>INTERNAL PHOTOS</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Operational Description</td>
<td>OPERATIONAL DESCRIPTION</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Schematics</td>
<td>CIRCUIT DIAGRAM</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Test Report</td>
<td>TEST REPORT</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Test Setup Photos</td>
<td>TEST SETUP PHOTOS</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Users Manual</td>
<td>MANUAL</td>
<td>10/02/2003</td>
<td>pdf</td>
<td>10/02/2003</td>
</tr>
</tbody>
</table>
Device Internals
cy7c63723 usb/ps2 microcontroller

24w02 serial eeprom
2k (256x8)
Device Reversing
Communication

• One way traffic (replay attacks!)
  – except kb
• No standard data protocol
• Varied RF protocols and frequencies.
  – 27 Mhz
  – 900 Mhz
  – 2.4 Ghz
Applications

- Wireless mouse
- Car alarm and home security systems
- Remote control systems
No text provided in the image.
Reversing the protocol

- One way messages must include
  - Authentication data (serial number)
  - Data
- Tap at the input to the TX Chip
  - No noise or errors
- Tap at the output of RX to verify and build the sniffer.
Reversing the Protocol

Page Down
0111110 1010 1110 0110 0100 1001 0101 0010 1000001

Page Up
0111110 1010 1110 0110 0100 1101 0101 0110 1000001

“Hide”
0111110 1010 1110 0110 0100 1011 0101 1010 1000001
Reversing the Protocol

Page Down
0111110 1010 1110 0110 0100 1001 0101 0010 1000001

Page Up
0111110 1010 1110 0110 0100 1101 0101 0110 1000001

“Hide”
0111110 1010 1110 0110 0100 1011 0101 1010 1000001
Reversing the Protocol

Page Down
1010 1110 0110 0100 1001 0101 0010

Page Up
1010 1110 0110 0100 1101 0101 0110

“Hide”
1010 1110 0110 0100 1011 0101 1010
Reversing the Protocol

Page Down
1010 1110 0110 0100 1001 0101 0010

Page Up
1010 1110 0110 0100 1101 0101 0110

“Hide”
1010 1110 0110 0100 1011 0101 1010
Reversing the Protocol

Page Down
1010  1110  0110  0100  1001  0101  0010

Page Up
1010  1110  0110  0100  1101  0101  0110

“Hide”
1010  1110  0110  0100  1011  0101  1010
# Reversing the Protocol

<table>
<thead>
<tr>
<th>header</th>
<th>serial</th>
<th>data</th>
<th>serial</th>
<th>data</th>
<th>footer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0111110</td>
<td>xxxx  xxxx  xxxx  xxxx</td>
<td>xxxx</td>
<td>xxxx</td>
<td>xxxx</td>
<td>01001</td>
</tr>
</tbody>
</table>
Attacks
BYOM (bring your own MCU)

• Ideally the original MCU would be reprogrammed
  – Most are OTP (One time programmable)
  – Can’t read them, security fuse blown
• Our own MCUs are needed
Sniffing at the chip level
Injecting at the chip level
Passive attacks

• Needed to acquire authentication data
• Sensitive data from keyboards (passwords)
• Mouse data not very useful
Active attacks

- Attacks are HID type dependent
  - Keyboards (including presenters)
  - Mice
Active Keyboard Attacks

+ ‘R’ == (:
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: [ ]
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: iexplore http://www.attackersmachine.com|
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: `cmd`
While at the cmd ...

Echo data to a bat file

Run the bat file
Active Mouse Attacks

What can be done by being able to inject mouse movement and clicks?

- Being able to see the screen. (Attacking a live presentation)
- Blind
Accessibility for the Attacker
Blind Attacks

- No visual feedback.
- Educated guessing
- Mouse movement scripting
Getting Feedback

- Attempt to connect to controlled webserver
- Check logs
- Readjust and reattack
Microcontrollers
More MCU uses

- Custom bit stream sniffer/recorder/interface
- Custom bit generator driven by software
Future Work

• Keyboards
• Scripting interface
• Software controlled bit generation
Thank you for flying from San Francisco International, a world-class Airport dedicated to serving the “City by the Bay”.

NOTIFICATION OF INSPECTION (NOI)

In order to protect you and your fellow passengers, Covenant Airport Security (CAS) is required by law to inspect all checked baggage. CAS is a private company under contract with the Transportation Security Administration (TSA) to provide baggage and passenger screening at San Francisco International Airport.

As part of this process, your bag was identified for physical inspection. If your bag was locked using non-TSA recognized locks, CAS may have had to break the locks. If prohibited items, including Hazardous Materials, were discovered during an inspection, they were turned over to the appropriate authorities.

Furthermore, in order to ensure the highest quality of service, CAS employees are continuously monitored by either direct supervision or cameras surveillance.

We appreciate your understanding and cooperation. For questions and guidelines, feel free to contact us during your next trip or to learn how to report a claim, please visit cassecurity.com or call 1-866-338-1580 from 8:00 AM to 5:00 PM PST.

Covenant NOI 126365
Flight UA 474
Summary

- Find FCC ID info
- Tap into data path.
- Reverse the protocol
- Inject/Sniff data using customized MCUs
- Client enforced security is still client enforced security
Questions?

luis@ringzero.net