IRON-HID:
Create your own bad USB

Seunghun Han
Who am I?

- Security researcher at NSR (National Security Research Institute of South Korea)
- Operating system and firmware developer
- Author of the book series titled “64-bit multi-core OS principles and structure, Vol.1 & 2”
- a.k.a kkamagui (crow or raven in English) - @kkamagui1
Contents

- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of a Smartphones
- Testing a Vulnerability of a POS System and a PC
- Bonus
• Background and Architecture of IRON-HID

• Hacking a Portable Charger

• Testing a Vulnerability of the Smartphone

• Testing a Vulnerability of the POS System and the PC

• Bonus
IRON-HID Project?

IRON-HID

Human Interface Device for making your tools
Features

- Custom device + firmware + test agent program + Android smartphone program
- Various types of system exploitable
  - POS (Point-of-Sale), PC, Android, etc.
- Lightweight embedded hardware-based
  - “Arduino” and “Teensy”
- Open-source project!
  - https://github.com/kkamagui/IRON-HID
# Arduino vs Teensy

<table>
<thead>
<tr>
<th>Arduino</th>
<th>Teensy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arduino Mega</td>
<td>Teensy++ 2.0</td>
</tr>
<tr>
<td>Larger (Palm size)</td>
<td>Smaller (Paper-clip size)</td>
</tr>
<tr>
<td>256KB Flash (ATmega16U2 + ATmega2560)</td>
<td>128KB Flash (AT90USB1286)</td>
</tr>
<tr>
<td>60 I/O Pins</td>
<td>46 I/O Pins</td>
</tr>
</tbody>
</table>

Arduino Sketch IDE is available!
Target POS systems, PCs, smartphones

Test agent (TA) program

Send commands and events
Install a test agent program

Receive results of commands
(Results of shell, screens, files)

Custom device
(in proxy devices)

IRON-HID firmware
(USB functions and a CD-ROM image)

Embedded hardware
(Low-powered hardware)

Wireless module
(WiFi, Bluetooth, Cellular, etc.)

Execute shell commands
Send keyboard events
Capture screens
Get files

Receive results of commands
Receive status of a proxy device

Security inspector’ smartphone
IRON-HID commander program

: IRON-HID component
IRON-HID Firmware

- Emulates **keyboard and mass-storage device**
  - It has one interrupt type endpoint for sending and logging keyboard events
  - It has two bulk type endpoints for installing the TA program

- Makes a custom **communication channel**
  - It has one control type endpoint for making a tunnel between the TA program and the Commander program
TA program and IRON-HID Commander

- TA program processes requests of Commander
  - Command Executions, Screen Captures, File Transfers

- Commander is an interface of pen-testers
  - It has control tab, command tab, key tab
  - Penetration tester uses each tab for testing security holes
<table>
<thead>
<tr>
<th>Direction</th>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commander → TA program</td>
<td>C;&lt;command&gt;;</td>
<td>Commander requests that TA program executes a <strong>command</strong> and sends result to Commander</td>
</tr>
<tr>
<td>Commander → TA program</td>
<td>G;&lt;filename&gt;;</td>
<td>Commander requests that TA program sends a <strong>file</strong> to Commander</td>
</tr>
<tr>
<td>Commander → TA program</td>
<td>S;;</td>
<td>Commander requests that TA program captures a <strong>screenshot</strong> and sends it to Commander</td>
</tr>
<tr>
<td>TA program → Commander</td>
<td>F;;&lt;64byte data&gt;;</td>
<td>TA program sends <strong>results</strong> to Commander</td>
</tr>
<tr>
<td>Commander → Firmware</td>
<td>&lt;Magic string 1&gt;</td>
<td>Commander changes <strong>firmware’s mode</strong> to command transfer mode</td>
</tr>
<tr>
<td>Commander → Firmware</td>
<td>&lt;Magic string 2&gt;</td>
<td>Commander changes <strong>firmware’s mode</strong> to keyboard event mode</td>
</tr>
<tr>
<td>Commander → Firmware</td>
<td>&lt;Magic string 3&gt;</td>
<td>Commander requests that firmware installs <strong>TA program</strong> into host</td>
</tr>
<tr>
<td>Firmware → Commander</td>
<td>M;;&lt;keyboard event&gt;;</td>
<td>Firmware sends user’s <strong>keyboard inputs</strong> to Commander</td>
</tr>
<tr>
<td>Firmware → Commander</td>
<td>D;;&lt;debug message&gt;;</td>
<td>Firmware sends <strong>debug messages</strong> to Commander</td>
</tr>
</tbody>
</table>
We are ready to launch!

Choose a target to attach it
We want a portable charger

- We use the smartphone everywhere!!
  - We spend much time with the smartphone
  - But, it doesn’t have enough battery
  - So, you should bring your charger or …
So many portable chargers...
So many battery rental services...
Hey,
You totally believe your portable charger?
PowerShock!!

- It is a portable charger, but not normal
  - It has IRON-HID inside it
- It can test Android smartphones
- It can test POS(Point-Of-Sale) Systems
- It can test your PC

It is a perfect weapon for penetration testers
• Background and Architecture of IRON-HID

• Hacking a Portable Charger

• Testing a Vulnerability of the Smartphone

• Testing a Vulnerability of the POS System and the PC

• Bonus
Tools you need
Inside of the portable charger

- It has a very simple architecture
  - A charger module and battery cells
  - High capacity model → More battery cells!
Cutting off battery cells

- Make some space for IRON-HIDs
  - Battery cells are connected in parallel
  - Cut off the cell connector carefully
Pin layouts of the charger module

USB Connector for Input (recharging)

- VCC (No.5)
- ID (No.1)
- Data+ (No.1)
- Data- (No.1)

USB Connector for Output (smartphone)

- GND (No.4)
- Data+ (No.1)
- Data- (No.1)
- VCC (No.1)
### USB Datasheet

<table>
<thead>
<tr>
<th>Micro Type</th>
<th>A Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Micro Type Diagram" /></td>
<td><img src="image2" alt="A Type Diagram" /></td>
</tr>
<tr>
<td><strong>No.1</strong> (VCC)</td>
<td><img src="image3" alt="VCC" /></td>
</tr>
<tr>
<td><strong>No.5</strong> (GND)</td>
<td><img src="image4" alt="GND" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mini Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image5" alt="Mini Type Diagram" /></td>
</tr>
<tr>
<td><strong>(VCC)</strong></td>
</tr>
<tr>
<td><strong>(GND)</strong></td>
</tr>
</tbody>
</table>

Dimensions:
- **Micro Type**
  - Width: 7.9
  - Height: 2.5
- **A Type**
  - Width: 5.12 ± 0.10
  - Height: 1.07 ± 0.042
- **Mini Type**
  - Width: 3.95 ± 0.156
Pin layouts of the IRON-HID

### Teensy
- GND
- VCC
- D (Data+)
- D (Data-)

### Bluetooth Serial Module (RN-42 Silver)
- VCC
- GND
- TX
- RX
- RTS
- CTS

### Comparison

<table>
<thead>
<tr>
<th>Teensy</th>
<th>Bluetooth</th>
</tr>
</thead>
<tbody>
<tr>
<td>5V OUT</td>
<td>VCC</td>
</tr>
<tr>
<td>D2 (RX)</td>
<td>TX</td>
</tr>
<tr>
<td>D3 (TX)</td>
<td>RX</td>
</tr>
<tr>
<td>GND</td>
<td>GND</td>
</tr>
</tbody>
</table>
You got the power!!

* Rebirth of the Portable Charger *
USB OTG (On-The-Go)

- It activates the USB host function of smart-phones
  - You can connect various types of USB peripherals such as a keyboard, a mass-storage (USB drive), a mouse

* The final piece of the puzzle *
THIS IS NOT WHAT I WANT
Making a custom OTG cable

Connect the ID pin with the GND pin.
• Background and Architecture of IRON-HID

• Hacking a Portable Charger

• Testing a Vulnerability of the Smartphone

• Testing a Vulnerability of the POS System and the PC

• Bonus
Well-known Smartphone Vulnerability

Do you use a pattern lock?  
Yes

Do you set a backup PIN?  
Yes

Can you type backup PINs unlimitedly?  
Yes

You are in danger

You are safe (maybe...)

Try again in 14 seconds.

Emergency call

Backup PIN
Testing the vulnerability

- Connect **PowerShock** to a smartphone with the custom **OTG cable** and fire!!
  - It is really hard to test the vulnerability with your hands
  - The PowerShock tests it instead of you
    - It sends PINs quickly and automatically!!

If someone asks you to charge a phone, charge it with **PowerShock!!**
Demo

(Let’s test the Android)
Background and Architecture of IRON-HID

Hacking a Portable Charger

Testing a Vulnerability of the Smartphone

Testing a Vulnerability of the POS System and the PC

Bonus
Many POS systems are PC-based!!
If the PowerShock plugs into the POS?

If POS system has a vulnerability, you can grab card numbers!!
Demo

(Let’s test the POS system)
• Background and Architecture of IRON-HID
• Hacking a Portable Charger
• Testing a Vulnerability of the Smartphone
• Testing a Vulnerability of the POS System and the PC
• Bonus
KeyboardShock

Attach IRON-HID onto USB keyboards and give them to your colleagues.
Find the key matrix with multimeter
The example of the keyboard matrix

<table>
<thead>
<tr>
<th>Rows</th>
<th>Columns</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td>LGUI</td>
<td></td>
<td></td>
<td>ESC</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>RCONTROL</td>
<td></td>
<td></td>
<td>RSHIFT</td>
<td></td>
<td></td>
<td>Z</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>LCONTROL</td>
<td></td>
<td></td>
<td>LSHIFT</td>
<td>TILDE</td>
<td>F1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q</td>
<td></td>
<td>W</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>6</td>
<td>RGUI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rows</td>
<td></td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>F4</td>
<td></td>
<td>G</td>
<td>H</td>
<td>F6</td>
<td>F5</td>
<td>QUOTATION</td>
</tr>
<tr>
<td>2</td>
<td>C</td>
<td></td>
<td>V</td>
<td>M</td>
<td>COMMA</td>
<td>PERIOD</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td></td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>F2</td>
<td></td>
<td>5</td>
<td>6</td>
<td>EQUAL</td>
<td>F8</td>
<td>MINUS</td>
</tr>
<tr>
<td>5</td>
<td>E</td>
<td></td>
<td>R</td>
<td>U</td>
<td>I</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>6</td>
<td>F3</td>
<td></td>
<td>T</td>
<td>Y</td>
<td>CLOSEBRAKET</td>
<td>F7</td>
<td>OPENBRAKET</td>
</tr>
<tr>
<td>7</td>
<td>D</td>
<td></td>
<td>F</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>SEMICOLON</td>
</tr>
<tr>
<td>8</td>
<td>B</td>
<td></td>
<td>N</td>
<td></td>
<td></td>
<td></td>
<td>SLASH</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td></td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>Rows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>F5</td>
<td></td>
<td>ENTER</td>
<td>NUMLOCK</td>
<td>PAD_0</td>
<td>PAD_PERIOD</td>
<td>UP</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LALT</td>
</tr>
<tr>
<td>3</td>
<td>F10</td>
<td></td>
<td></td>
<td>F11</td>
<td>PAD_SLASH</td>
<td>PAD_ASTERISK</td>
<td>PAUSE</td>
</tr>
<tr>
<td>4</td>
<td>F9</td>
<td></td>
<td>DELETE</td>
<td></td>
<td>INSERT</td>
<td>PAGEDOWN</td>
<td>END</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PRINTSCREEN</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>BACKSPACE</td>
<td></td>
<td>PAD_7</td>
<td>PAD_8</td>
<td>PAD_9</td>
<td>PAD_PLUS</td>
<td>SCROLLLOCK</td>
</tr>
<tr>
<td>7</td>
<td>INVERSESLASH</td>
<td></td>
<td>PAD_4</td>
<td>PAD_5</td>
<td>PAD_6</td>
<td>APPLICATION</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SPACE</td>
<td></td>
<td>DOWN</td>
<td>RIGHT</td>
<td>PAD_MINUS</td>
<td>LEFT</td>
<td>RALT</td>
</tr>
</tbody>
</table>
ReaderShock

Attach IRON-HID onto card readers and give them also to your colleagues
Then...

You will be the big brother for fun!!

<table>
<thead>
<tr>
<th>CONTROL</th>
<th>COMMAND</th>
<th>KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C:&gt; notepad no-mercy.txt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C:&gt; format c: /q</td>
<td></td>
</tr>
</tbody>
</table>

Executing commands

Logging and sending keys

Receiving files and capturing screenshots
Resources

- http://www.fourwalledcubicle.com
- http://cdemu.blogspot.com
- http://www.usb.org
- https://www.arduino.cc
- https://www.pjrc.com/teensy
Thank you!

I will be waiting for your email
@kkamagui1, hanseunghun@nsr.re.kr