Universal RF USB Keyboard Emulation Device
URFUKED

-by Monta Elkins

monta.defcon @ geeks午餐.com
version .08 6/2010
Updates at: http://www.hackerwarrior.com/urfuked
Receiver
(plugged into spare USB port)

“Teensy”
Microcontroller

RF receiver
On the back

Quarter

• Receiver is very small
• Can be encased in plastic to look like a typical USB key
Pwner
portable, battery powered, rf transmitter

LEDs Show What Attack to Perform

Power Switch

Input Switch Set Attack

Ownzred Switch Transmits Attack
Hardware Construction
Teensy uc
Transmitter
Receiver
Antenna is 23 cm long

Use either of two Vcc pins on Teensy

Use either of two Ground Pins on Teensy (connect all receiver grounds)

Data Pin is D2

Receiver Construction

“Teensy” 2.0 Microcontroller
$18

Sparkfun RF Receiver 315 Mhz
$4.95

Construction consists of soldering 7 wires. Simple!
Pwner Construction
(rf transmitter)

“Front” View

“Teensy” Microcontroller
$18

Sparkfun RF Transmitter
$3.95

“Rear” View
Teensy Pins

Pin Assignments Using Arduino Software

- GND
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

(interior) AREF

(interior) 24

+5V

PWM

PWM INTO

INT1

RX

INT2

TX

INT3

PWM

PWM

PWM

GND

RST

(led on 11)
Pwner Schematic

LEDs

Pull # 0 1 2 3
Name B0 B1 B2 B3

"Send" "1" "0"

Switch 0 Switch 1 Switch 2

Pull # 2 1 0 19
Pin name F0 F1 F4 A0 A1 A2

F0, F1, F4 have internal pull-up resistors
Pwner Case
Pwner Case
Receiver Assembled
Live Demo
URFUKED opens the windows run dialog box using the keyboard shortcut “windows key” + R.

In this demo it runs the benign command “notepad.exe”- but any other valid command could be executed.
After opening the notepad.exe window, URFUKED types text into the window in this demonstration “attack”
Inspiration

Inspired by (Adrian Crenshaw) 
the IronGeek's:
Programmable HID USB 
Keystroke Dongle [PHUKD].

URFUKED overcomes the blind timing, and attack selection difficulties, by incorporating an RF transmitter and expands the concept to include multiple O.S. attacks.

[Adrian, I know you're here somewhere, Thanks! I owe you a beer.]
Interface Details
Using The Interface

First two lights represent O.S. to attack:

01 = Windows
10 = Mac
11 = Linux
00 = Mouse Attack
(for mouse attack the two attack lights represent length of attack)

Enter a “0”
Enter a “1”

These two lights represent the attack to perform:

00 = notepad message
01 = web page load
10 = download software
11 = rm -rf

Easily expandable to 64 different attacks.

Transmit Attack
Transmission Protocol
Transmission Frames

Receiver continually “receives” bytes even when there is no transmission due to ambient RF noise. I use these frames to distinguish a transmission from noise.

Valid Frame Definition:

- 3 Carrier Bytes (or more)  
- 0xAA
- Command Sequence Number  
- 0-127
- Command Byte  
- Any value
- Checksum  
- Command Sequence Number  
- + Command Byte
Transmission

For reliability the transmitter sends the following command frame 10 times for each command send button press.

• 10 Carrier Bytes
  0xAA
• Command Sequence Number
  0-127
• Command Byte
  Any value
• Checksum
  Command Sequence Number + Command Byte

Each command frame is repeated 10 times for redundancy - the command is only executed once by the receiver even if multiple valid copies are received due to the Command Sequence Number.
Software
Software Location

http://www.hackerwarrior.com/urfuked
Attack Scenarios
Scenarios

Exfiltrate information from the target
Infiltrate (plant) information on target computer
Install remote administration tool or virus on the target

Political style attacks
  Facebook postings
  In appropriate web browsing (in conjunction with mouse control

Disabling attacks
  rm -rf style
  Remove all files in home directory etc.

Financial Attacks
  Paypal transfer attack
  Ebay bid attack
Modifying Software for Unique Attacks
Key Selection
Sources
## Sources

<table>
<thead>
<tr>
<th>Part</th>
<th>Source</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td><a href="http://www.hvwtech.com/products_view.asp?id=1041">www.hvwtech.com/products_view.asp?id=1041</a></td>
<td>$4.95</td>
</tr>
<tr>
<td>Buttons, LED's, misc.</td>
<td><a href="http://www.digikey.com/">http://www.digikey.com/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.radioshack.com">http://www.radioshack.com</a></td>
<td></td>
</tr>
<tr>
<td>USB adapter</td>
<td><a href="http://www.dealextreme.com/details.dx/sku.2704~r.48687660">http://www.dealextreme.com/details.dx/sku.2704~r.48687660</a></td>
<td>$1.07</td>
</tr>
</tbody>
</table>