HAPPY HACKING

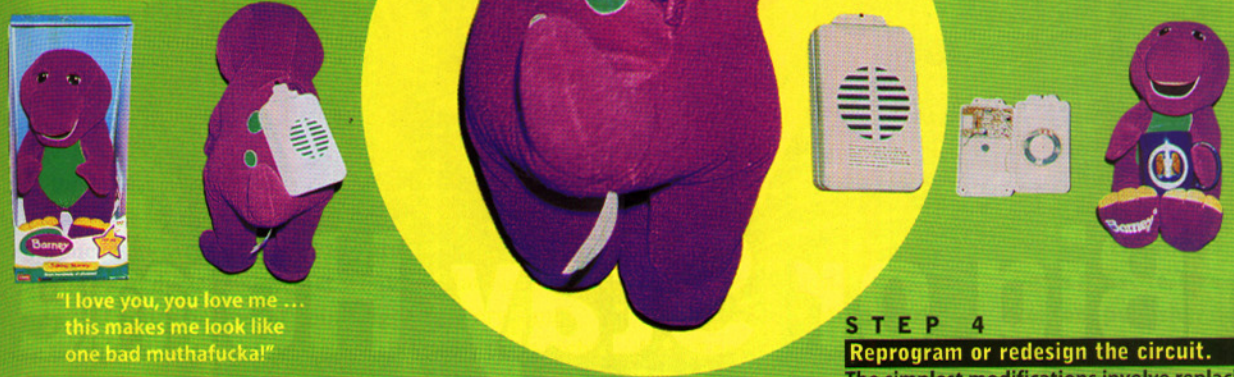
By Kingpin

Hacking a toy can be as fulfilling as infiltrating a large corporate computer system, as I've learned during my various adventures with Tamagotchi, Playskool Talking Barney, Texas Instruments's Speak & Spell, and various other playthings. Because most microcontroller-based toys use the same basic theory to direct their behavior, the following instructions can serve as a general guide for toy hacking:

STEP 1

Remove the control circuitry from the toy.

In most special feature plush toys, the electronic control system is located in the same small plastic box that contains the batteries. You can usually just pull the box out of the toy through a velcro slit in the fur that provides access to the battery compartment. If necessary, you can use a scalpel. Be careful not to break the wires leading from the box to any of the toy's "internals," such as the light, pressure, or sound sensors. The US$24.99 Playskool Barney I hacked had a four-wire connector that joined Barney's "brain" to two pressure switches located inside his hand and stomach.



"I love you, you love me ... this makes me look like one bad muthafucka!"

STEP 2

Develop a schematic.

Portable electronic toys are usually controlled by a 4-bit or 8-bit microprocessor, with some type of ROM/RAM to store and execute the software. You might find that yours has one or more black blobs on the circuit board. These are known as chip-on-board (COB) packages; one will probably serve as the CPU. (If you get lucky, your toy will have standard plastic packages for the CPU and/or ROM, rather than the smaller COB. The larger the component, the easier it is to experiment with.) You can begin developing a schematic simply by drawing the components and the connections among them. By following the connections between the CPU and the switches, sensors, and other external devices, you'll quickly be able to determine the I/O (input/output) pins. Once the schematic is complete, the toy's basic functions – and how to change them – will be much clearer.

STEP 3

Reverse-engineer the circuit.

With your schematic as a guideline, use an oscilloscope, logic analyzer, logic probe, or multimeter to monitor the signals coming to and from various pins on the CPU. If you know where the switches are connected, you can short the pins together with a screwdriver or wire to simulate a button press. By learning the function and behavior of the pins on the CPU, you should be able to learn how the toy operates.

The Playskool Barney has two COB packages. I first assumed that one COB was the microprocessor, the other, marked "U1", a voice-storage unit. The audio was formed by a frequency-modulated square wave generated by the CPU. (Simpler designs may use a set of resistors to form a simple, low-cost digital-to-analog converter to generate the audio.) Simulating a press of the "hug" button elicited such phrases as "You're stuupendous!" "You're super-d-dooper!" and "Remember – I love you!" When I pushed Barney's right hand, however, the CPU constructed sentences out of subsets of words in a seemingly random way. Very clever!

STEP 4

Reprogram or redesign the circuit.

The simplest modifications involve replacing the external switches with relays, transistors, or custom electronic designs. On Playskool Barney, for example, replacing the pressure switch in the tummy with an optical sensor will turn it into a sunrise-activated alarm-clock. If you know where the switch interfaces with the PC board, you can easily complete this hack. Getting more complex, you could swap address pins or exchange components.

I also added my own sound samples to Barney's internal circuitry. Using an ISD voice/record playback IC (RadioShack #276-1325, $17.99), I redesigned an entirely separate circuit board and connected it to the hand and tummy switches. Now, when someone squeezes Barney, he says things I recorded from *South Park*, including "This makes me look like one bad muthafucka."

Depending on the design, you can change the pitch, speed, or volume of the generated audio by replacing fixed resistors with a potentiometer (a variable resistor). Connecting certain pins to ground (or pulling them high) can also lead to interesting "features." The popular Tamagotchi toy, for example, can be made to last longer or grow stronger by resetting various internal pins.

Don't be afraid to experiment. And don't be afraid to damage components – the joy of hardware hacking is figuring out how things work. The manufacturers just want you to buy another toy, anyway. ■ ■ ■

Kingpin is a hardware hacker and one of the seven members of L0pht Heavy Industries (www.lopht.com/).