Dark Box
~~~~~~~~

The Dark Side Research Group

Proudly Presents:
The DARK BOX: Multi-Purpose Network Manipulation Unit

By: Cablecast 0perator

-=> Introduction <=-

The Dark Box is the newest device to enter the "colored box" market and is guaranteed to rerevoloutionize the art of telecommunications fraud. The device's inventor, Cablecast 0perator, became quite bored with the old forms of phreaking, having to worry about codes dying, or being traced. The unit you are about to build was spawned by the need for a more versitile, safe and interesting way to phreak. You don't need any special tones or attack dialers, just your good old every-day DTMF pushbutton phone.

The box's basic design allows you to call anywhere on earth (or elsewhere for all we care) without fear of being billed or traced. But it's uses do not stop there! When hooked up properly, it can be used to emulate multi-line bridges, loop lines and direct in-dials.

It's really quite simple. The device is plugged into two phone lines, other than your own, or one end into a phone line and the other into another box. When there is an incoming call, the device senses this and picks up the phone. Your call is then transferred to the other line or onto the loop. When you hang up, the device senses this, too, and it hangs up also, waiting for the next caller.

To illustrate this, whip out your good old analog multimeter and hook it up to your phone line. See that nice, juicy voltage on there? Now call it on your other line. The voltage will jump and the polarity will go all to hell. This version of the Dark Box uses an alternating current detector to tell if the phone is ringing because sensing voltage is unreliable and not entirely universal. Now pick up your second line. There is a momentary blackout on it and then the voltage becomes constant. Now hang up the phone you called in on. There will be another blackout on your other line ans then
~~~~~~~~

the voltage will pop back up again. On the box, hangup is detected by the line current passing through an optoisolator that is holding the relay open. When it is cut off for the split second the blackout occurs, the relay is cut off and the phone hangs up.

NOTE: With the rapid expansion of digital ESS's, the little phone company quirks that are essential for the device's operation might not be available in your area. Check your line with the meter as directed to be sure!

-=> Trip To Radio Snack <=-

On your next trip out to your friendly neighborhood Radio Shack, get yourself these:

1:1 Audio Isolation Transformer
555 IC Timer
Optoisolator (Transistor Output)
(2) NPN Transistors (2N3904 or 6 Will Do Nicely)
(2) 100k 1/4w Resistors
(2) Normal Diodes
1k 1/4w Resistor
10mF Electrolytic Capacitor
Disc Capacitor (.01mF)
DPST Relay
9v Battery or Likewise AC Adapter and Timer

It'll run you about five or six bucks, unless of course you get a five finger discount...It can be mounted on a small IC perfboard, or whatever you like depending on how small you want it.

If you can't display the schematic that goes along with this, we'll do it like connect the dots, it'll be fun!!

```
                                                                  +          O
P          Q
   _________           ________          ___|_____|_____|_____|___
A -|o              |- H   I -|o              |- N   |   C
|
B -|       555      |- G   J -|    OptoIs   |- M     |    O      DPDT/DPST
|
C -|    ICTimer |- F     K-|_______|- L       |     I          Relay
|
D -|________|- E                                  |_L______________________|
                                                                  |          |
|          |
```

- R

S T

*yea...you can make this schematic out....as good as I'm gonna make it

This is the wiring diagram for X1, the 1:1 Audio Transformer:

```
RED --(white)--------O||O--------------(red)-- YEL
                                        O||O
GRN --(black)--------O||O-----------(yellow)-- BLK
```

They don't have to be paired exactly like that, just remember that white goes with black, and red goes with yellow.

Text coding of the schematic is very simple. If you have ever assembled one of those 1,000,000,000,000-in-1 electronics kits from Shack, you can do this... I will guide you with TO and THRU. There is a difference:

```
 A ----*---- B          A ----- R1 ----- B
       |
       R1

 "A TO R1 TO B"            "A THRU R1 TO B"
Parallel Circuit           Series Circuit
```

These are the abbreviations for the components:

RED, GRN, YEL, BLK = Phone line red and green respectively
Dx(Anode/Cathode) = The Diodes Where x=1,2
Qx(Emitter/Base/Collector) = Transistors x=1,2
C1(+/-) = Electrolytic Capacitor (observe polarity!)
C2 = Disc Capacitor
R1 = 1k Resistor
Rx = 100k Resistor x=2,3

Ya dig it, mon? If this is too complex for you, try and view the schematic through Generic Software's CADD, or try to draw your own out from the directions below. Sometimes it helps to do this in visual terms!

Ok, let's go to it...

<-=->
1: GRN thru R3 to Q1(Emitter) to GND
2: RED thru D1(Anaode) to Q1(Base)
3: Q1(Collector) to B

```
 4: +V thru R1 to B
 5: +V to M to D to H to Q2(Collector)
 6: H thru R2 to G to F thru C1(+) to GND
 7: E thru C2 to A to GND
 8: C thru D2(Anode) to Q2(Base) to L
 9: Q2(Emitter) thru COIL to GND
10: RED to I
11: J thru X1 to T
12: GRN to R
13: BLK thru X1 to Q
14: YEL to O
<-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=->
```

There. That wasn't too hard now, was it? Now let's test it. A word to the wise: Do not substitute batteries or other power supplies in place of the telephone line. If you do, then you risk blowing the transformer and the optoisolator.

-=> Testing The Puppy <=-

Now that you have it built, double check and make sure everything is OK before you apply power to it. If everything you have is right, there might be some wierd, uncaught error in the file, or you have bad parts. Contact us or try again.

A voltmeter and a logic probe can come in handy here...

Connect the battery, but not the phone line yet. Your relay should not throw. If it does, check the 555 and the transistor triggering it.

If that's ok, short out the emitter and collector on Q1 momentarily. The relay should throw for about two or three seconds then shut off. If not, check that trigger circuit again.

Now plug in RED and GRN. If your relay trips, you might have the RED and GRN reversed, or Q1 is not wired properly.

If you're ok, call it on your other line. It should ring once and then pick up. If it's busy, perhaps D1 is not right. If it doesn't answer the phone, check Q1 to make sure all contacts are right.

Ok, FINAL TEST! Connect YEL and BLK and call the line that RED and GRN are on. It should pick up and you should hear a steady dial tone and be able to dial DTMF on it, etc etc etc. There are several problems that could arise here. 1) No dial tone means it's either not hooked up right, or the transformer is bad. 2) If you only get it for about three seconds before it hangs up on you, you are not getting complete isolation from the other line. Check the transformer. 3) If the dial tone you hear is "bobbled" then you have a major voltage spillover, isolate the second line from the rest of the circuit.

If everything checks out, you have just built a DARK BOX!! Now let's have fun with it...

-=> Applications And Operations <=-

You already have the basic unit constructed. This is sort of a Pseudo-Extender or Pseudo-Diverter. Place it on any two phone lines (other than your own) and be sure you know the number for the RED-GRN pair. Now when you call the line that's hooked up to RED and GRN, you get the dial tone from the YEL/BLK pair, and it's just like you were at that person's house using THEIR phone! But you're not, you could be in Tahiti if you want! This is, basically, how you avoid billing of calls.

If you want to use this box from long distance without having to pay for it yourself, you could wire a black box resistor onto the RED/GRN pair. It's not your phone line, what do you care?

For loop lines and cheese boxes, wire two Dark Boxes back to back on any two phone lines.

For a multiple line bridge, you need as many boxes as you want dial-ins. Loop all the YEL's and BLK's together respectively and plug the RED/GRN's into a hunt group (You know, call 555-0000 and if it's busy, you'll be transferred to 555-0001, etc etc), this way, hackers can drop in and out at will. Didn't Cap'n Crunch do something like this?

If you want to make credit card calls instead of dialing direct, attach the box to two payphones that are next to each other. That way, you don't have to freeze your ass off to avoid having your phone number put on the guy's card bill. Make sure the payphones will accept incoming calls!

Patch YEL/BLK into an audio amplifier and into the paging system at someplace like K-Mart. Imagine the riot you can start by paging "INS! Stay where you are!" The xfrmer should push out a line level audio, so interfacing to most sound applications should be a snap.

A word about Caller ID. CI has been introduced scince the invention of the box. The box can bypass CI to an extent, being that if the box calls someone who caller ID's you, they'll get the second phone line of the box, and not you. However, if the indialing line for the box has CI and you call directly into it and someone happens to be there to get it, you could be in serious trouble. A soloution to this would be to use the box on a payphone that will accept incoming calls. Scince noone gives a fuck who calls a pay phone, chances are it won't CI'd. You could also place the box in an area that doesn't have CI, whereas in order for CI to work, both the caller and the callee must be in service areas.

Don't be limited by only these suggestions! Be creative and let us know how you use it! Make a DID for your school's PABX, or get your VICModem to autoanswer! There HUNDREDS of uses for this revoloutionary device waiting to be discovered!

-=> One Final Word <=-

The staff of Dark Side Research would like to thank our friend, Rebecca, who has encouraged us to press on in the Box's development even during times when it seemed hopeless.

Enjoy you new toy....

Cablecast 0perator