JOSHUA BRASHARS

and the
RAIDERS of the
LOST PHONES

Exploit Archaeology

First in the series of talks on excavating and exploiting retro hardware.

I promise the talk will get technical.

Who am I?

- Penetration Tester
- Geek Dad
- Amateur Phone Phreak
- @savant42 on the twitters

Who I’m not.

- Leet.
- A programmer.
- A reverse engineer-er.
- A speller.

Why this talk?

From 50lb Weight to Stealth Attack Platform

Methodology > Results

The Journey

And to see if I could.

First Off...

Traveling with a Payphone is a giant pain in the ass.

Anyway.

Payphones used to be like this.

Nowadays they're like this.

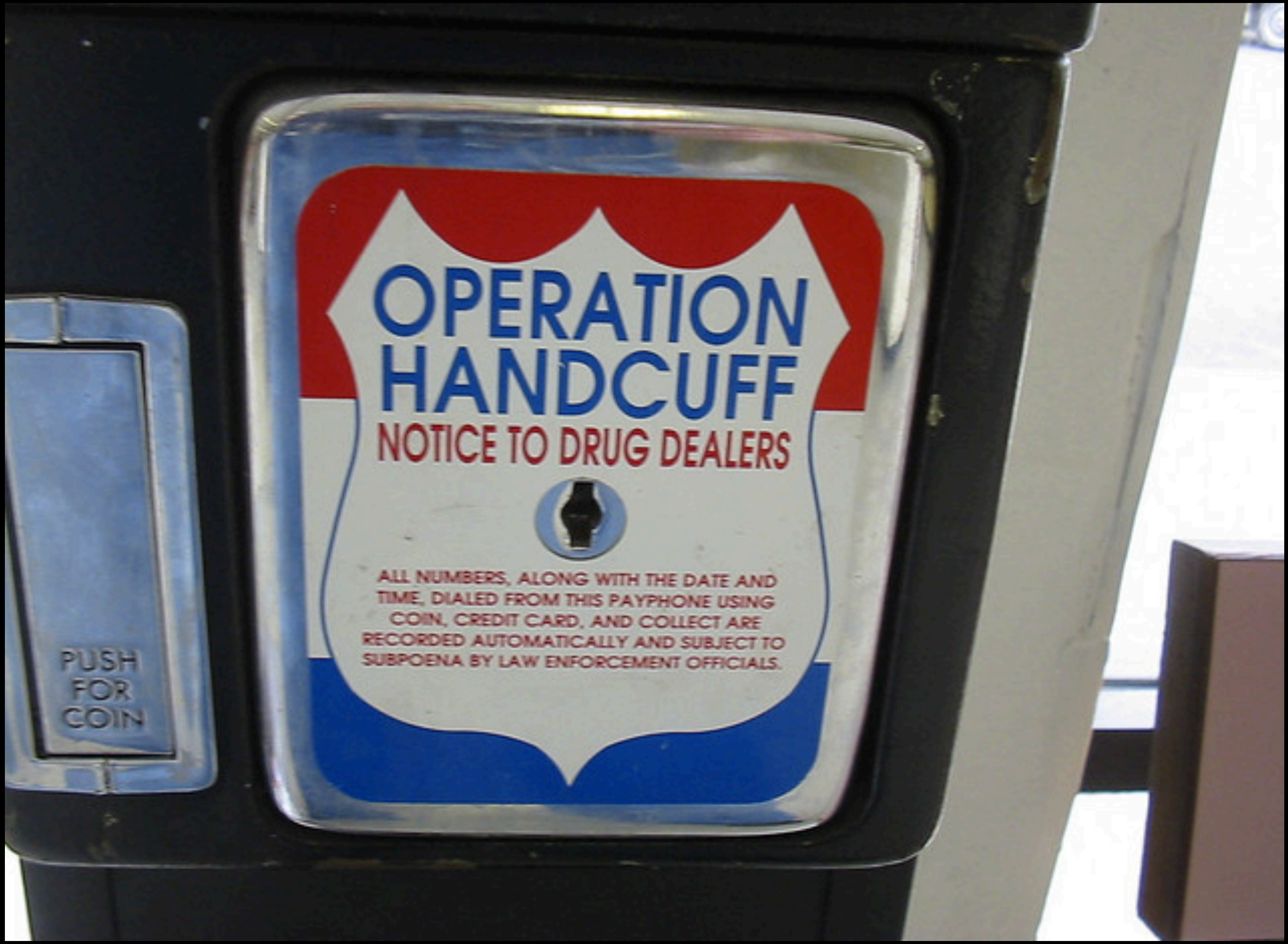
Phone

262
CALL THEM ALL
Your Cell Phone Charges You For Toll
CALL THEM ALL
FREE CALLS!! MAKE THEM HERE!!
GOODE PLUMBING
800-662-1875
FREE CALLS!! MAKE THEM HERE!!

If you see a payphone in your neighborhood today, you laugh.

If you see someone using a payphone?

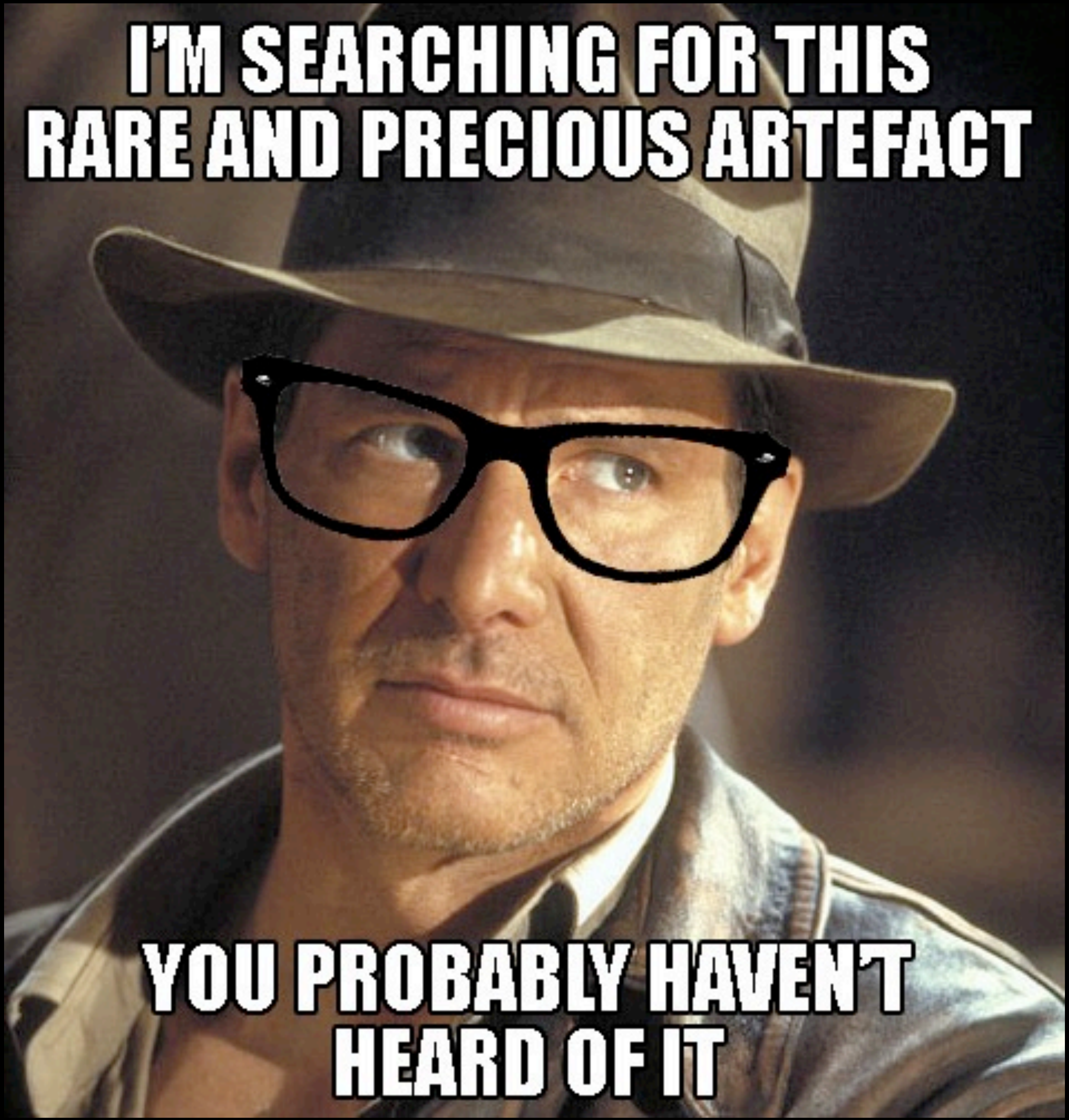
You lock your car doors and roll up the windows.


PUSH FOR COIN
OPERATION HANDCUFF
NOTICE TO DRUG DEALERS
ALL NUMBERS, ALONG WITH THE DATE AND TIME, DIALED FROM THIS PAYPHONE USING COIN, CREDIT CARD, AND COLLECT ARE RECORDED AUTOMATICALLY AND SUBJECT TO SUBPOENA BY LAW ENFORCEMENT OFFICIALS.

Even Indy is over it.

Ever since I was a kid

I’ve always wanted my very own payphone


I'M SEARCHING FOR THIS RARE AND PRECIOUS ARTEFACT
YOU PROBABLY HAVEN'T HEARD OF IT

One day, I got one as a gift.

(Thanks Tiffany & Gene Erik)

Still popular in correctional facilities

This one came from a prison. No joke.

(Yes, I cleaned the ever loving shit out of it)

BOCOT vs. COCOT

- BOCOT = Bell Owned Coin Operated Telephone (Telco Owned)
- COCOT = Customer Owned Coin Operated Telephone (Private)

Bell Owned

BOCOTS could be “Red Boxed” (utilize inband ACTS tones to signal coin insertion)

It’s probably still possible in certain regions of the US but most RBOCs have outsourced to private companies.

COCOT Payphones can not be Red Boxed without Operator Intervention (as far as *I* know) because they don’t use ACTS

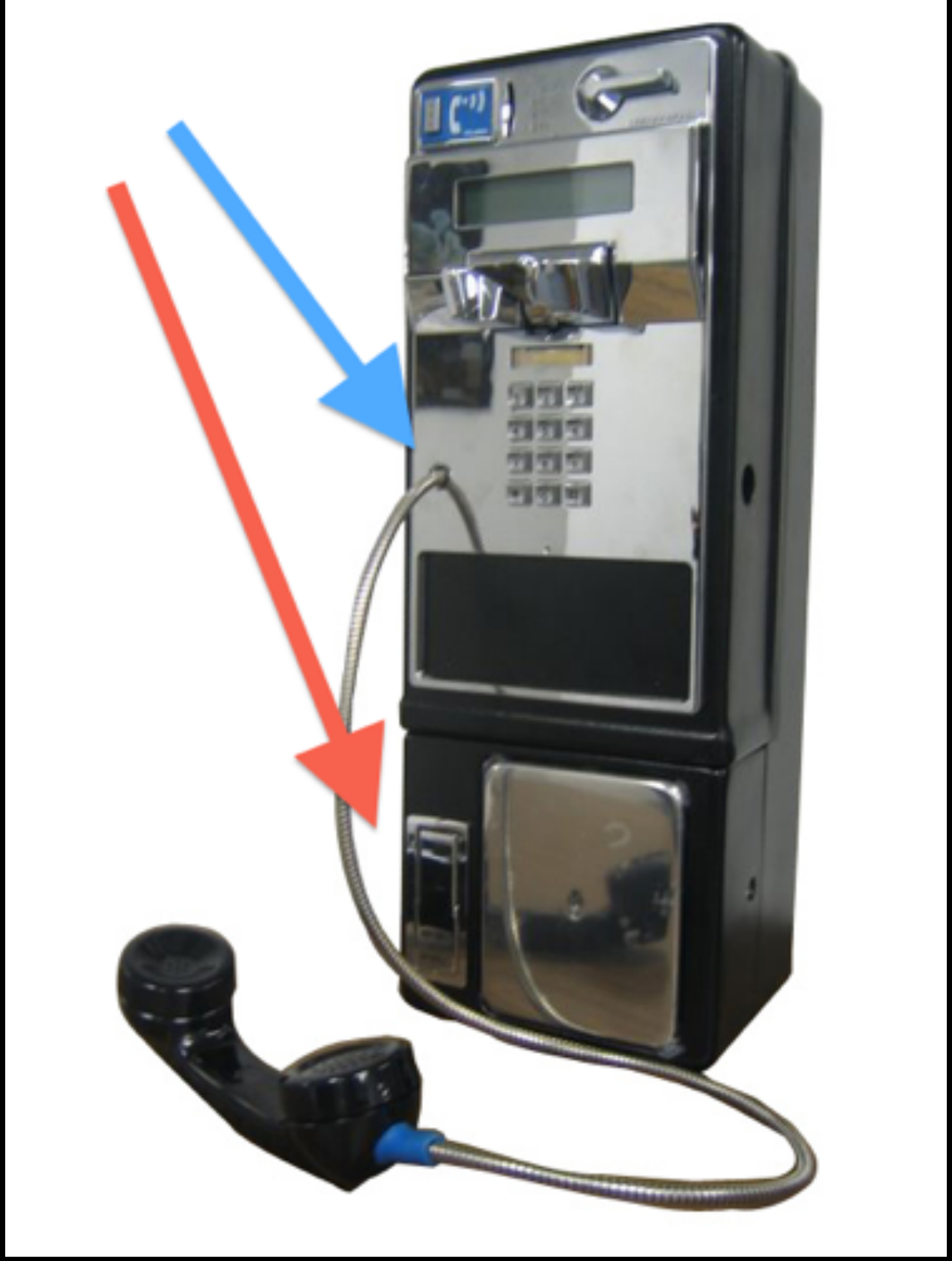
With “Smart Payphones” all of the call regulation, coin counting and management, etc, is done inside the payphone.

Telco payphones do all the magic at the Central Office.

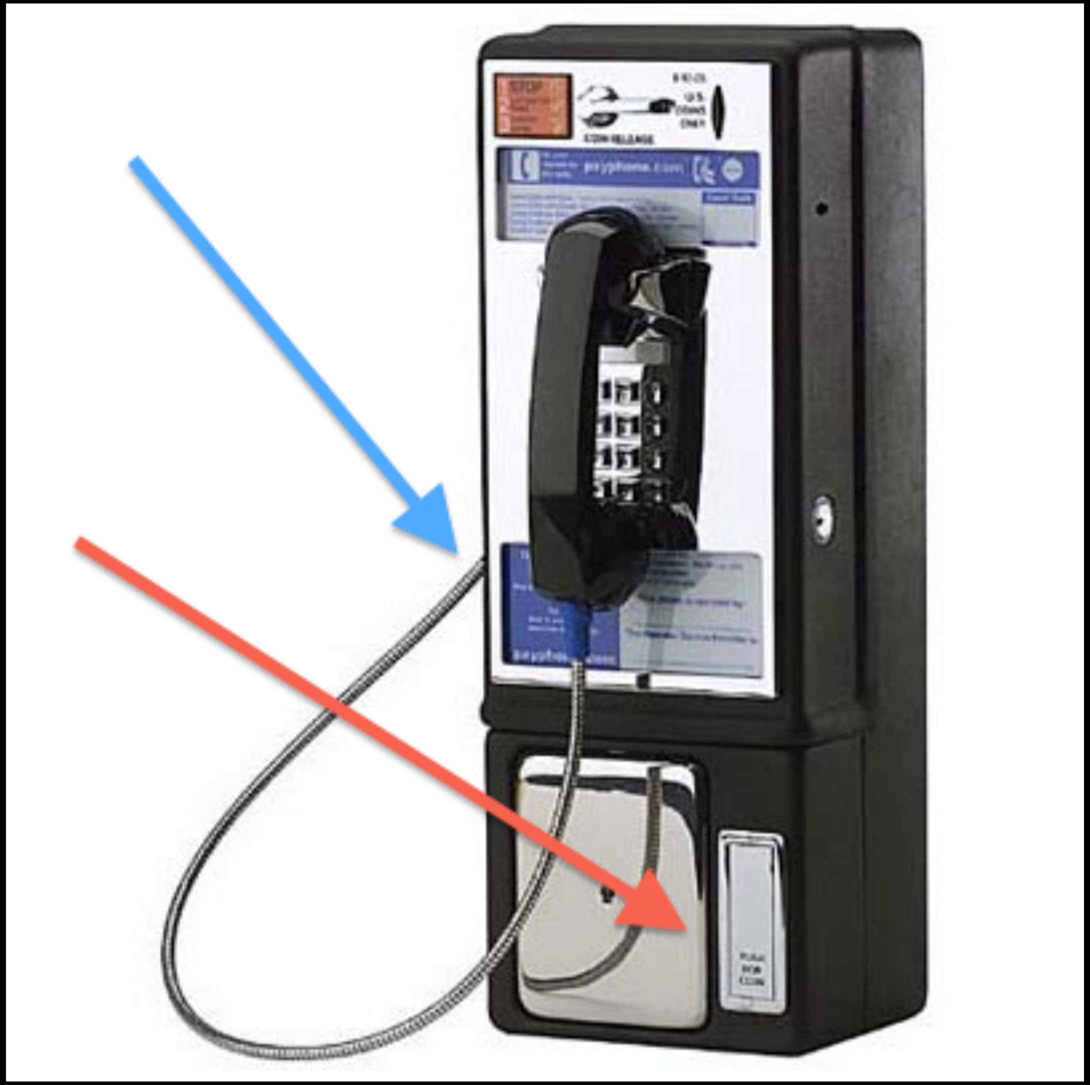
Telling the difference?

Most (All?) BOCOT Payphones use the General Electric style housing

Coin Return is on the Left and the armored cable connects to the front of the housing.



COCOTS often use the GTE style housing with the coin return slot on the right and the armored cable connects on the side. This is definitely not always the case, though.



This Payphone.

Elcotel Series 5 Line-Powered Payphone

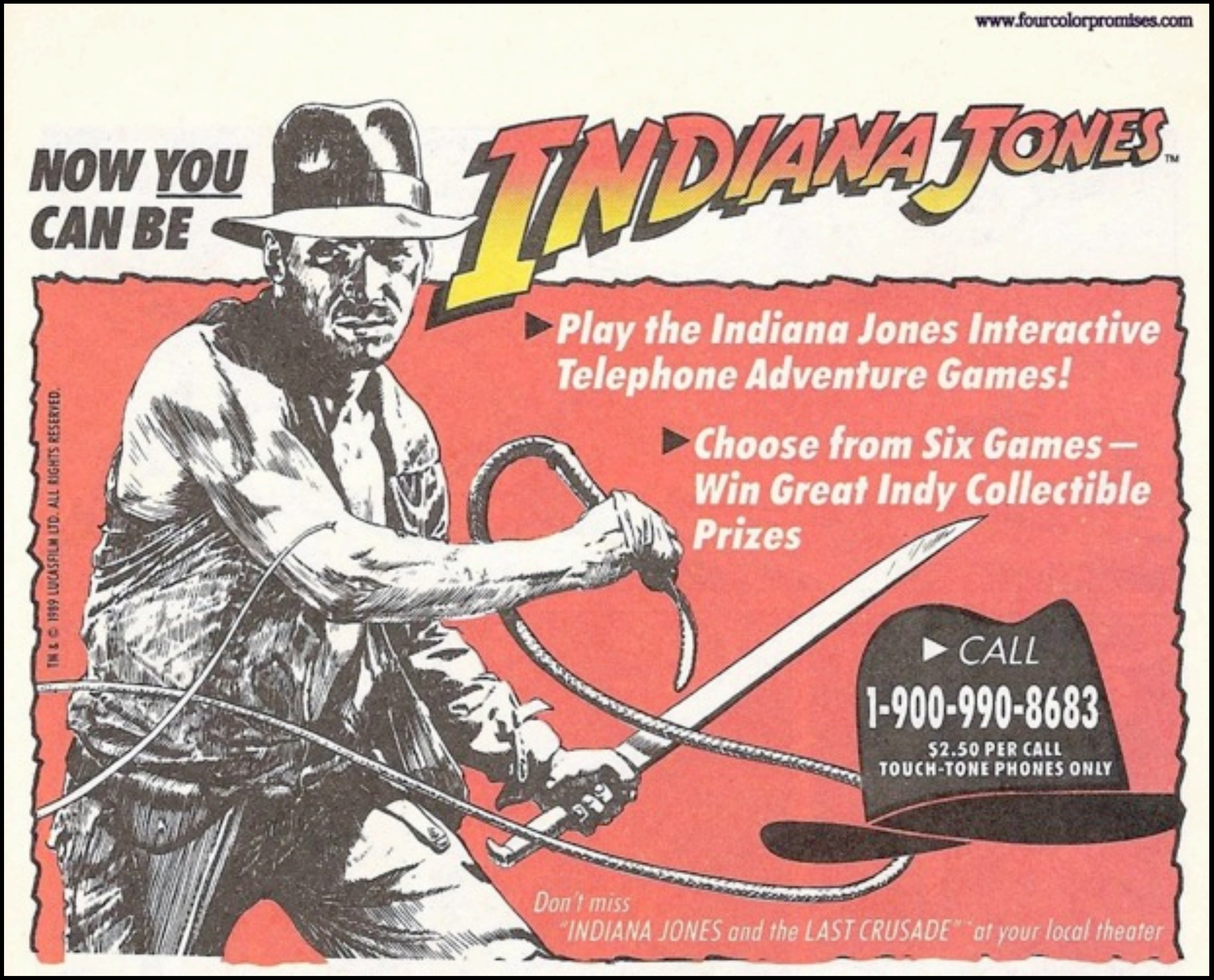
Internal Battery, trickle charges from voltage on the telephone line

“Smart” Phone, Programming/Rates are handled internal to the Payphone

Elcotel used to be prolific with the private coin phone market

Now they’re all but gone from most places

Now that I have one



www.fourcolorpromises.com

NOW YOU CAN BE INDIANA JONES™

► Play the Indiana Jones Interactive Telephone Adventure Games!

► Choose from Six Games — Win Great Indy Collectible Prizes

► CALL

1-900-990-8683

$2.50 PER CALL
TOUCH-TONE PHONES ONLY

Don't miss "INDIANA JONES and the LAST CRUSADE"™ at your local theater

TM & © 1989 LUCASFILM LTD. ALL RIGHTS RESERVED.

Problem?

No keys.

No battery.

No documentation.

Phone was from different area code.

How to do?

Get the phone open

Replace the battery

Reprogram for free calls.

Opening the phone

Milwaukee
18 VOLT
POWER-PLUS

Milwaukee
18 VOLT
POWER-PLUS

Preserving the tomb.

No destructive entry, wanted to keep the phone as intact as possible.

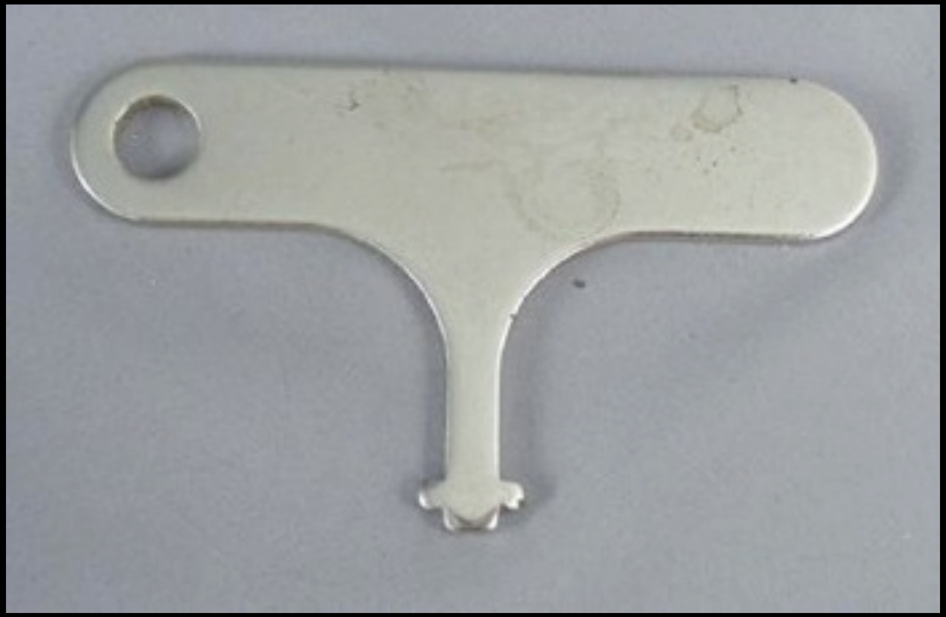
Three types of Keys

Upper Housing

Lower housing (coin vault)

T wrench for torque.

You need all three.



Upper Housing Lock

3 pins, no security Pins. Easy enough to pick in a short period of time.

Anti-impressioning divots.

Note: These locks tend to only rotate a quarter of a turn or less. Check, you may have already picked it.

Coin Vault Lock?

Not so much.

4 Pins, several spool pins.

Medeco Locks, though not biaxial

At that time, I was unable to pick it.

Hacker Con

Took the phone to Bay Threat in Mountain View

30 people tried, failed.

Except one guy.

Dude picked this lock in 10 seconds, by accident. Fuuuuuuuuuu.

Opening the housing

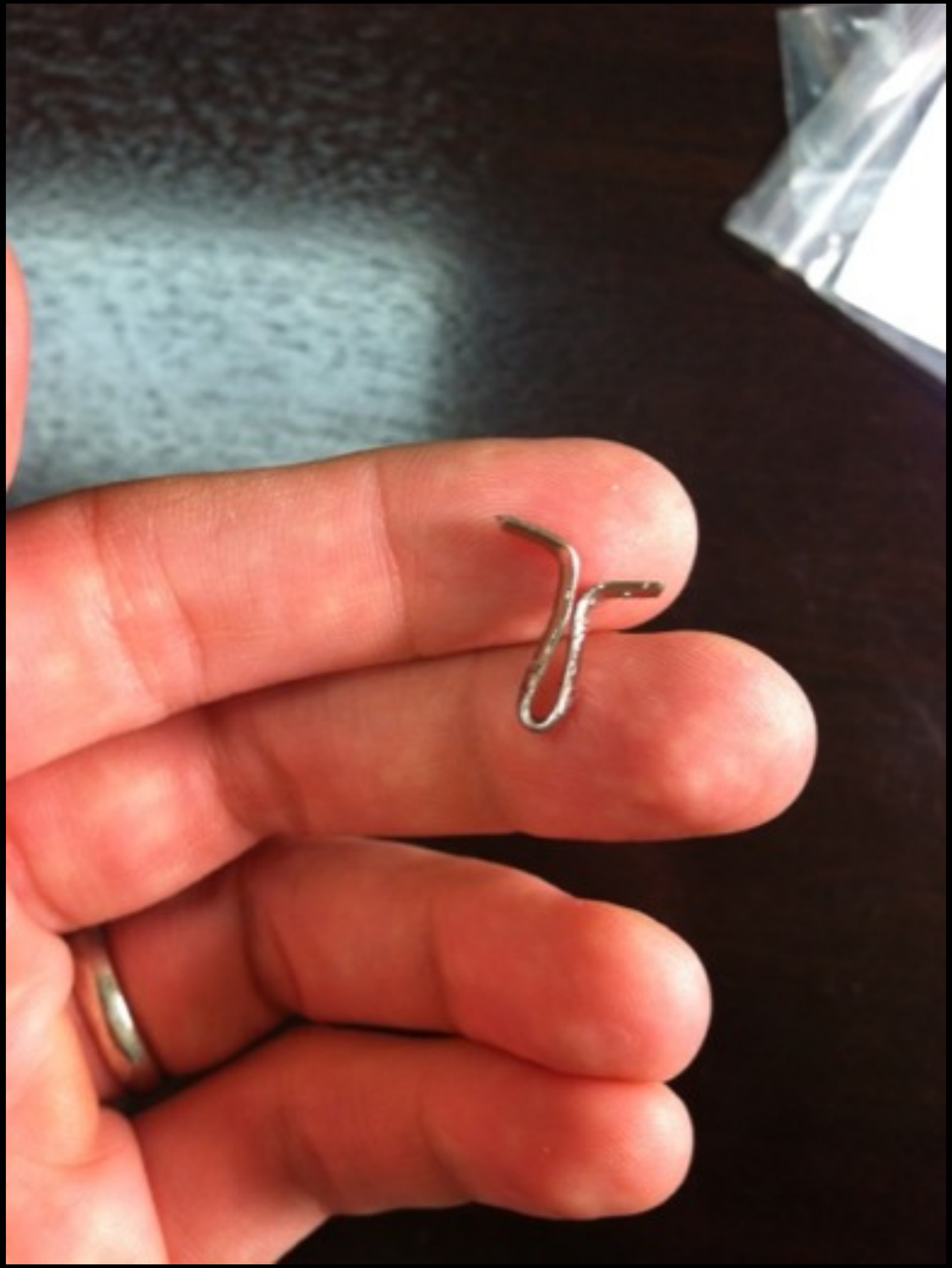
Didn’t have a T wrench, time to hack harder.

Opening the housing

Vyrus001 and I were able to hack something together.

Badge clip, wrench, faith.

Opening the housing



COIN RELEASE
U.S. COINS ONLY
No coin needed for SOS and free calls

Dead battery.

Payphone.com

u mad bro?

Now that it is alive

How the @#%#% do I use it?

How to do?

Different area code means local (to me) calls were $$$$$$$

Unacceptable.

GOALS:

The goals:

- Zero out the rates tables to make free calls
- Find vulnerabilities in payphone software
- ...
- Profit?

First Hack:

Payphone -> ATA -> Asterisk -> 911

Payphones are legally required to make 911 a free call.

Dial plan magic allowed me to get a usable dial tone if I first dialed 911.

Neat hack, but sloppy.

Documentation?

Nearly non-existent.

Archive.org was helpful, to an extent.

I learned how to reset phone to default, but that’s pretty much it.

Elcotel?

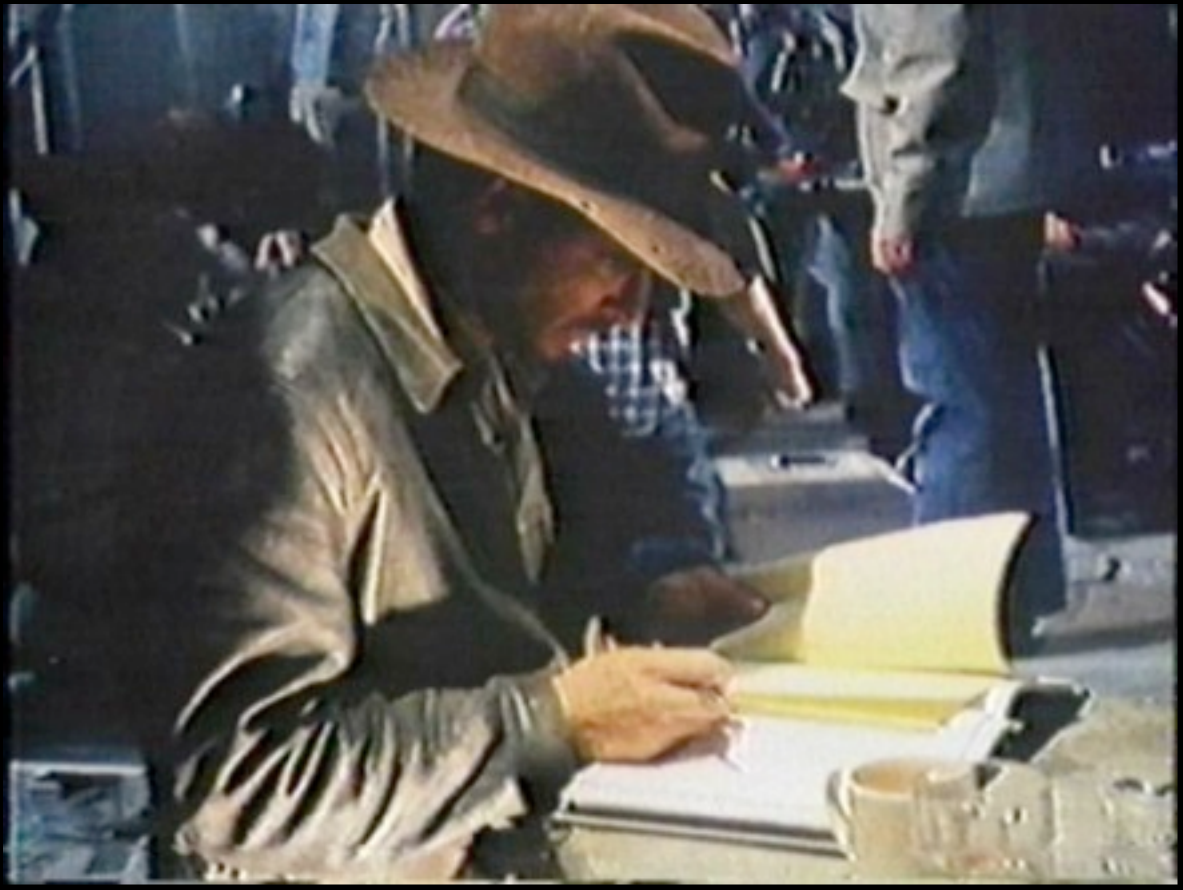
Ebay!

Incomplete.

Was only able to find part 2 of a 3 part series of manuals.

Basically, this was the rosetta stone.

Part 2 was useful, but I still didn't have the software to reprogram it.



3 Ways to Program:

- 1. Software based reprogramming
- 2. Local telemetry
- 3. Remote Telemetry

Software

Ideal solution, but requires the software and a license from a dead company.

Local Telemetry

- Open the Phone (which WILL set off alarms and call the phone owner if you try this in the field)
- Default the Phone
- Listen to voice prompts and dial to set values.

Remote Telemetry

Can allegedly reprogram remotely? (More on this later)

Software based programming

Eventually I was able to acquire a demo through “alternative means.”

Time to try and crack the software.

Cracking 10 year old software is actually pretty hard.

16-bit Windows "NE" Binary

Even IDA Pro was all "WTF Mate?"

I had a lot of help.

And by “help”, I mean that someone did it for me.

Eventually able to hook the installer, jump the serial number check, uncompress the installer archives.

Thanks to Vyrus001, int0x80, Frank^2

Phone has onboard modem called a "PCM" (Payphone Control Module)

Need to be able to dial it though.

Ironically, I don't have a landline.

Voice over IP

Unlocked Linksys Analog Telephone Adapter (ATA)

USB Modem

Voip Settings

- Dial up modem over VoIP is a pain in the ass.
- Ulaw or Alaw, accept no substitions.
- Disable Noise Cancellation + Echo suppression
- Really slow, ~ 9600 baud

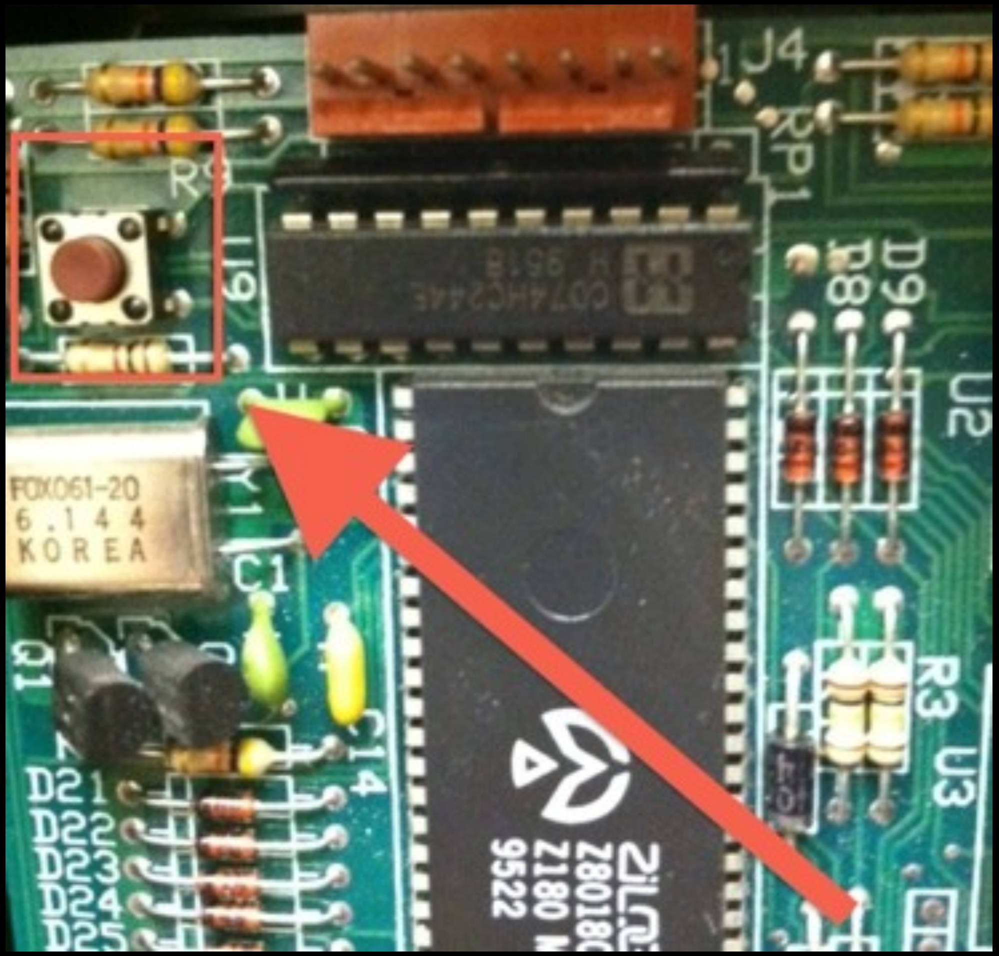
A HUGE Thanks! to the Telephreak guys (Hi Beave!) and the Oldskoolphreak.com guys for helping me get this sorted out.

Default the phone

Press and hold the button inside the phone.

Flash the hook.

Listen to onboard prompts



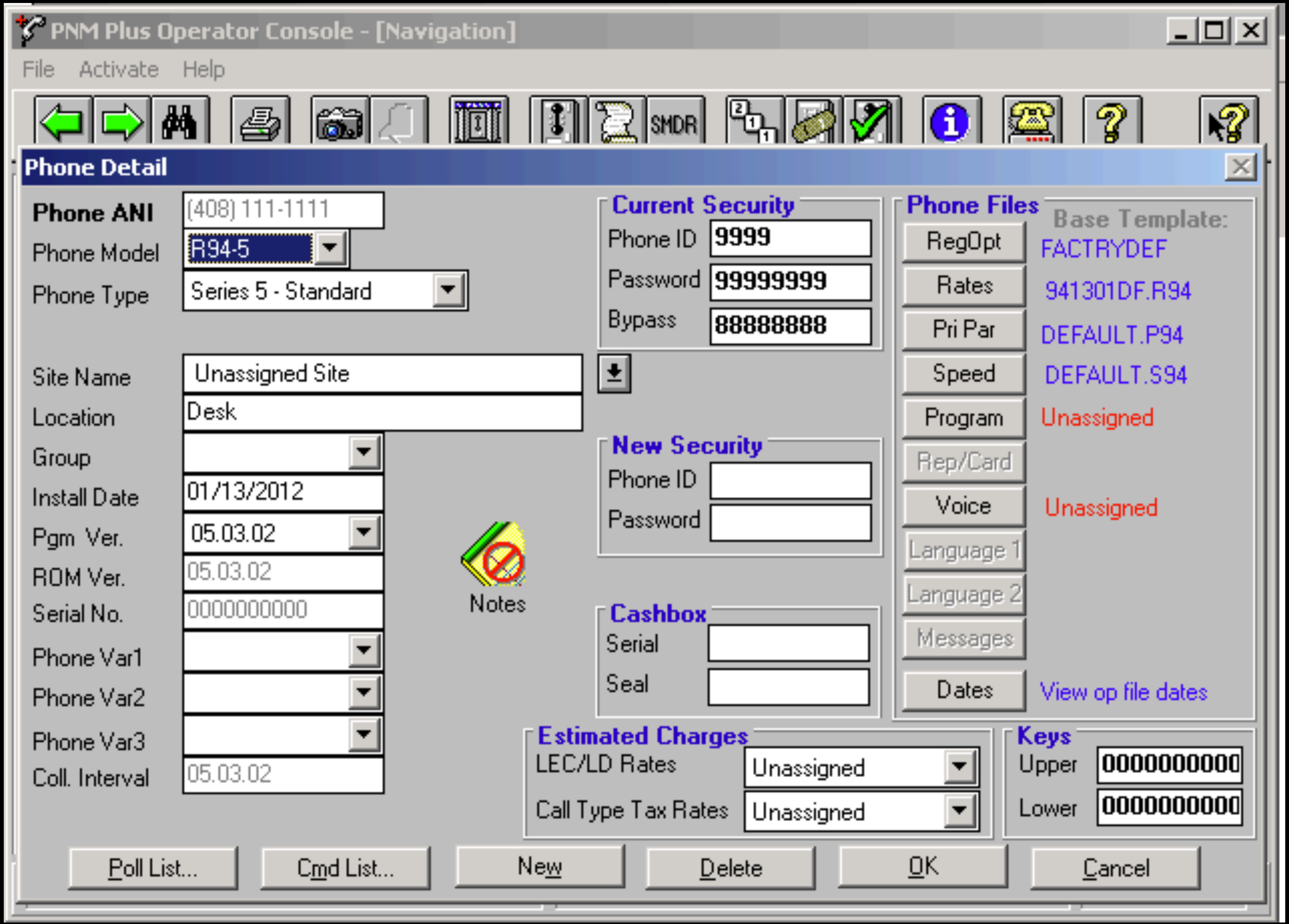
Local Telemetry

Press the button, flash the hook, enter the code, follow the voice prompts.

Super easy, but requires you to physically open the phone.

If the phone is not yours, this is dubious.

Now we can connect.



Phone Detail

Phone ANI: (408) 111-1111
Phone Model: R94-5
Phone Type: Series 5 - Standard

Site Name: Unassigned Site
Location: Desk
Group:
Install Date: 01/13/2012
Pgm Ver.: 05.03.02
ROM Ver.: 05.03.02
Serial No.: 0000000000
Phone Var1:
Phone Var2:
Phone Var3:
Coll. Interval: 05.03.02

Current Security
Phone ID: 9999
Password: 99999999
Bypass: 88888888

New Security
Phone ID:
Password:

Cashbox
Serial:
Seal:

Phone Files — Base Template:

RegOpt	FACTRYDEF
Rates	941301DF.R94
Pri Par	DEFAULT.P94
Speed	DEFAULT.S94
Program	Unassigned
Rep/Card	
Voice	Unassigned
Language 1	
Language 2	
Messages	
Dates	View op file dates

Estimated Charges
LEC/LD Rates: Unassigned
Call Type Tax Rates: Unassigned

Keys
Upper: 0000000000
Lower: 0000000000

Once you are able to connect, the rest is pretty easy.

But this talk is also about hacks, not using software.

Elcotel Engineers? Not total idiots.

Anti-fraud Mechanisms:

- Secondary Dialtone Detection
- Red box detection
- Chassis Alarms
- Brute Force Protection

Need to build a harness to fuzz the phone.

Intercept modem audio?

- Easy enough with SIP, but then what?

FSK Demodulation is crazy hard.

Blackbox RE of Protocol

If I could intercept and analyze how the software does it, I can do it myself.

How do I hook a USB Modem?

Advanced Serial Port Monitor Pro

- http://www.aggsoft.com/serial-port-monitor.htm
- Able to treat USB Modem as virtual serial port
- “Spy Mode” allows you to pass through and watch
- Displays output in either Hex or ASCII

Password?

Default password for software reprogramming is 99999999

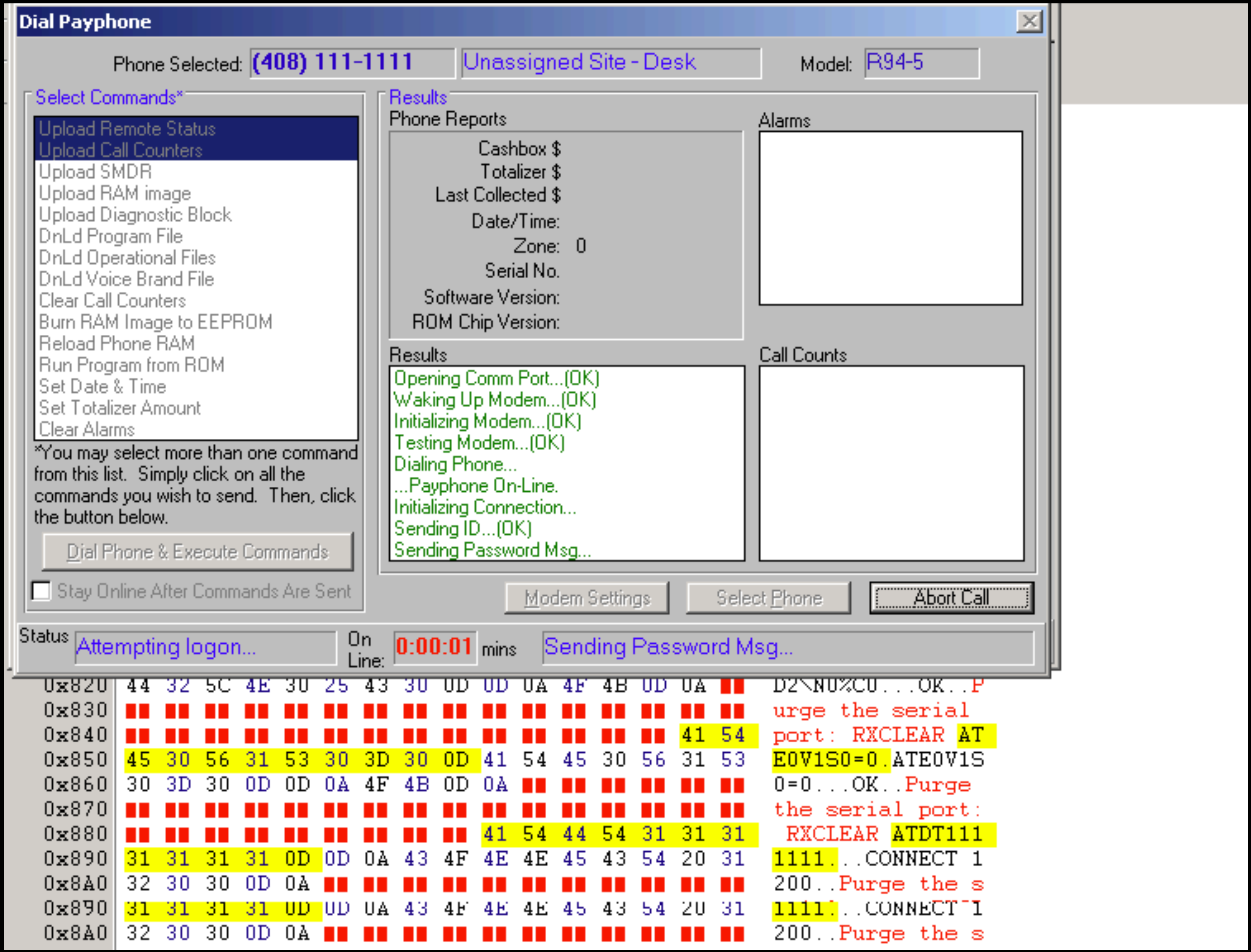
Default password for local and remote telemetry is 88888888

Performing actions using the PNM Plus Elcotel application enabled me to see what actions look like in Hexadecimal

From there I was able to make *some* sense of how the handshake worked

Phone ID is usually the last 4 digits of the phone number.

Passwords are almost never changed from defaults.



Phone Selected: (408) 111-1111 Unassigned Site - Desk Model: R94-5

Select Commands*

- Upload Remote Status
- Upload Call Counters
- Upload SMDR
- Upload RAM image
- Upload Diagnostic Block
- DnLd Program File
- DnLd Operational Files
- DnLd Voice Brand File
- Clear Call Counters
- Burn RAM Image to EEPROM
- Reload Phone RAM
- Run Program from ROM
- Set Date & Time
- Set Totalizer Amount
- Clear Alarms

*You may select more than one command from this list. Simply click on all the commands you wish to send. Then, click the button below.

□ Stay Online After Commands Are Sent

Results

Phone Reports

Cashbox $
Totalizer $
Last Collected $
Date/Time:
Zone: 0
Serial No.
Software Version:
ROM Chip Version:

Alarms

Results

```
Opening Comm Port...(OK)
Waking Up Modem...(OK)
Initializing Modem...(OK)
Testing Modem...(OK)
Dialing Phone...
...Payphone On-Line.
Initializing Connection...
Sending ID...(OK)
Sending Password Msg...
```

Call Counts

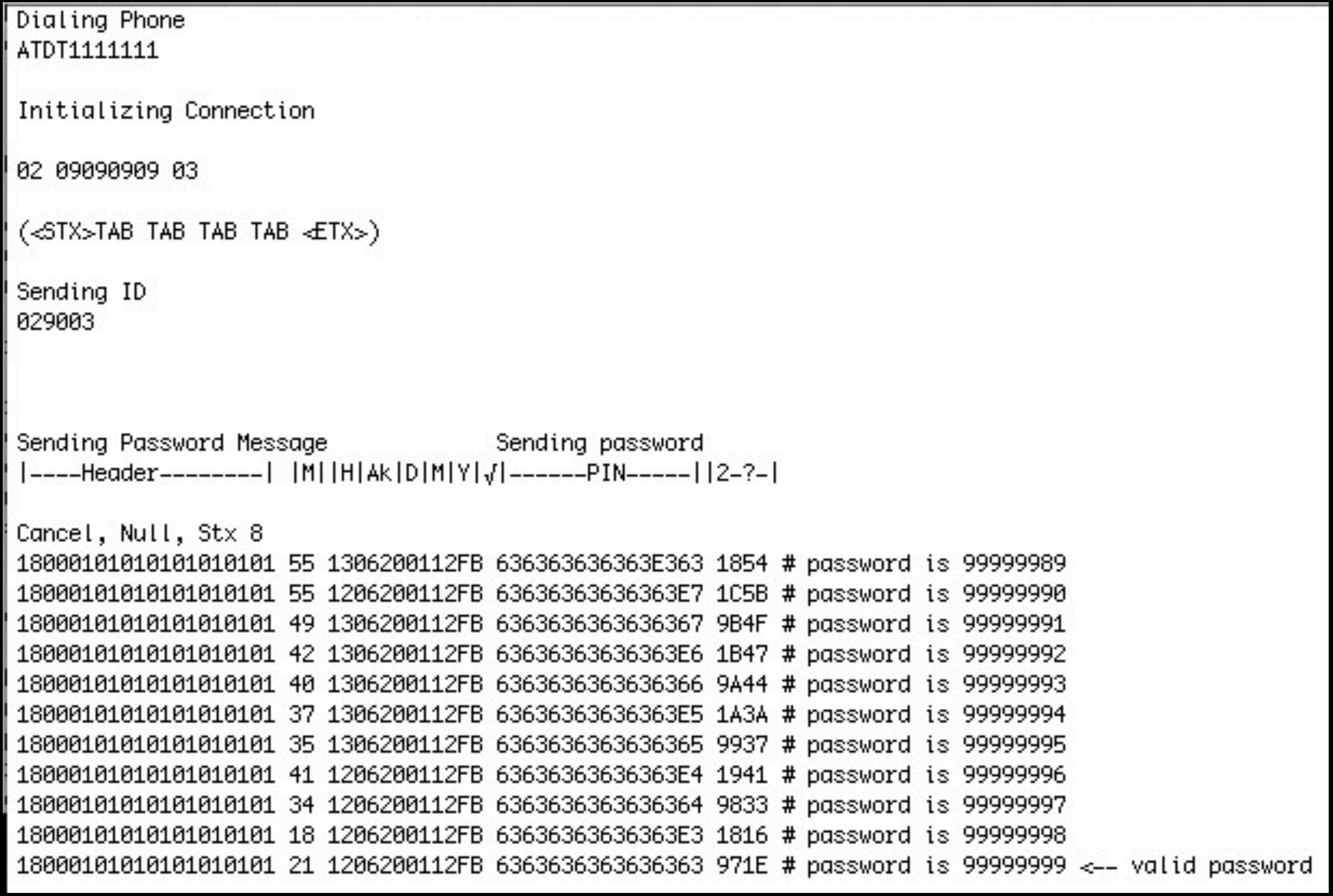
Status Attempting logon... On Line: 0:00:01 mins Sending Password Msg...

```
0x820  44 32 5C 4E 30 25 43 30 0D 0D 0A 4F 4B 0D 0A ■■  D2\N0%C0...OK..P
0x830  ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■  urge the serial
0x840  ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ 41 54  port: RXCLEAR AT
0x850  45 30 56 31 53 30 3D 30 0D 41 54 45 30 56 31 53  E0V1S0=0.ATE0V1S
0x860  30 3D 30 0D 0D 0A 4F 4B 0D 0A ■■ ■■ ■■ ■■ ■■ ■■  0=0...OK..Purge
0x870  ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■  the serial port:
0x880  ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ 41 54 44 54 31 31 31   RXCLEAR ATDT111
0x890  31 31 31 31 0D 0D 0A 43 4F 4E 4E 45 43 54 20 31  1111...CONNECT 1
0x8A0  32 30 30 0D 0A ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■  200..Purge the s
0x890  31 31 31 31 0D 0D 0A 43 4F 4E 4E 45 43 54 20 31  1111...CONNECT 1
0x8A0  32 30 30 0D 0A ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■ ■■  200..Purge the s
```

Demo

Oh dear $deity please work.

Auth Protocol Breakdown



```
Dialing Phone
ATDT1111111

Initializing Connection

02 09090909 03

(<STX>TAB TAB TAB TAB <ETX>)

Sending ID
029003



Sending Password Message            Sending password
|----Header--------|  |M||H|Ak|D|M|Y|√|------PIN-----||2-?-|

Cancel, Null, Stx 8
18000101010101010101 55 1306200112FB 636363636363E363 1854 # password is 99999989
18000101010101010101 55 1206200112FB 63636363636363E7 1C5B # password is 99999990
18000101010101010101 49 1306200112FB 6363636363636367 9B4F # password is 99999991
18000101010101010101 42 1306200112FB 63636363636363E6 1B47 # password is 99999992
18000101010101010101 40 1306200112FB 6363636363636366 9A44 # password is 99999993
18000101010101010101 37 1306200112FB 63636363636363E5 1A3A # password is 99999994
18000101010101010101 35 1306200112FB 6363636363636365 9937 # password is 99999995
18000101010101010101 41 1206200112FB 63636363636363E4 1941 # password is 99999996
18000101010101010101 34 1206200112FB 6363636363636364 9833 # password is 99999997
18000101010101010101 18 1206200112FB 63636363636363E3 1816 # password is 99999998
18000101010101010101 21 1206200112FB 6363636363636363 971E # password is 99999999 <-- valid password
```

Success vs. Fail

- When authentication fails, the Phone sends a hexadecimal NAK (Negative Acknowledgement)
  - 0x15
- When authentication is successful, Phone sends hexadecimal ACK (Acknowledge)
  - 0x06

Problem.

After 3 invalid attempts, the phone drops the call.

However, the PNM software is responsible for interpreting the “disconnect” message.

If we use our own code we can ignore that and keep trying until we get the right PIN.

Hacks.

Pseudo Code:

```
PIN = 0000
send $PIN
while ($auth_response != 0x06)
$PIN++
send $PIN
if $auth_response = 0x06, print “GREAT SUCCESS!”
```

Python has a good serial interaction library, but I don't code because I'm an idiot.

So Gene Erik jumped in.

Man I love having smart friends.

https://github.com/savantdc949/

Code will be online some time after Defcon hangover clears.

- User ID? Check.
- Pin? Check.
- ...
- Proft?

Enter: Remote Telemetry

- Call payphone from any landline phone
- Wait 30 seconds for Modem to stop screaming at you
- Have 10 seconds to enter telemetry password
- Listen to voice prompts

Reprogramming using DTMF (Remote Telemetry)

- Registers = Strings
- Options = On or Off
- Reg. 421-434 = Antifraud. Set to 0 to disable.
- Reg. 333-336, 412, and 414 = Disable alarms

More registers

- 404 = Phone number
- 402 = Phone ID#
- 403 = PNM Plus Password
- 400 = Telemetry Password
- 116 = Disable battery (DoS)
- 338 = Number for service desk

Service Desk

- Sudo/Operator status for Payphones
- If you divert this number to yourself, you can do cool stuff.
  - Apply credit
  - Issue refunds
  - Force phone to dial number for free
  - Dump the coin escrow ($$$$)

We can set the “coin escrow” to $5.

As people use the phone, up to $5 in coins collect in the escrow hopper.

Service desk can cause hopper to empty into coin return slot.

Demo?

Now what?

How can we use this information in a novel way?

ProjectMF

Blue Box simulation of Inband signalling over TDM trunks.

www.projectmf.org

Red Boxing

- Use sox and Asterisk EAGI to record and analyze inbound audio.
- Filter out all frequencies that are not 1700 Hz and 2200 Hz tones together
- If not null, incremend $coin_value
- If $coin_value >= $.25, make call

Now what?

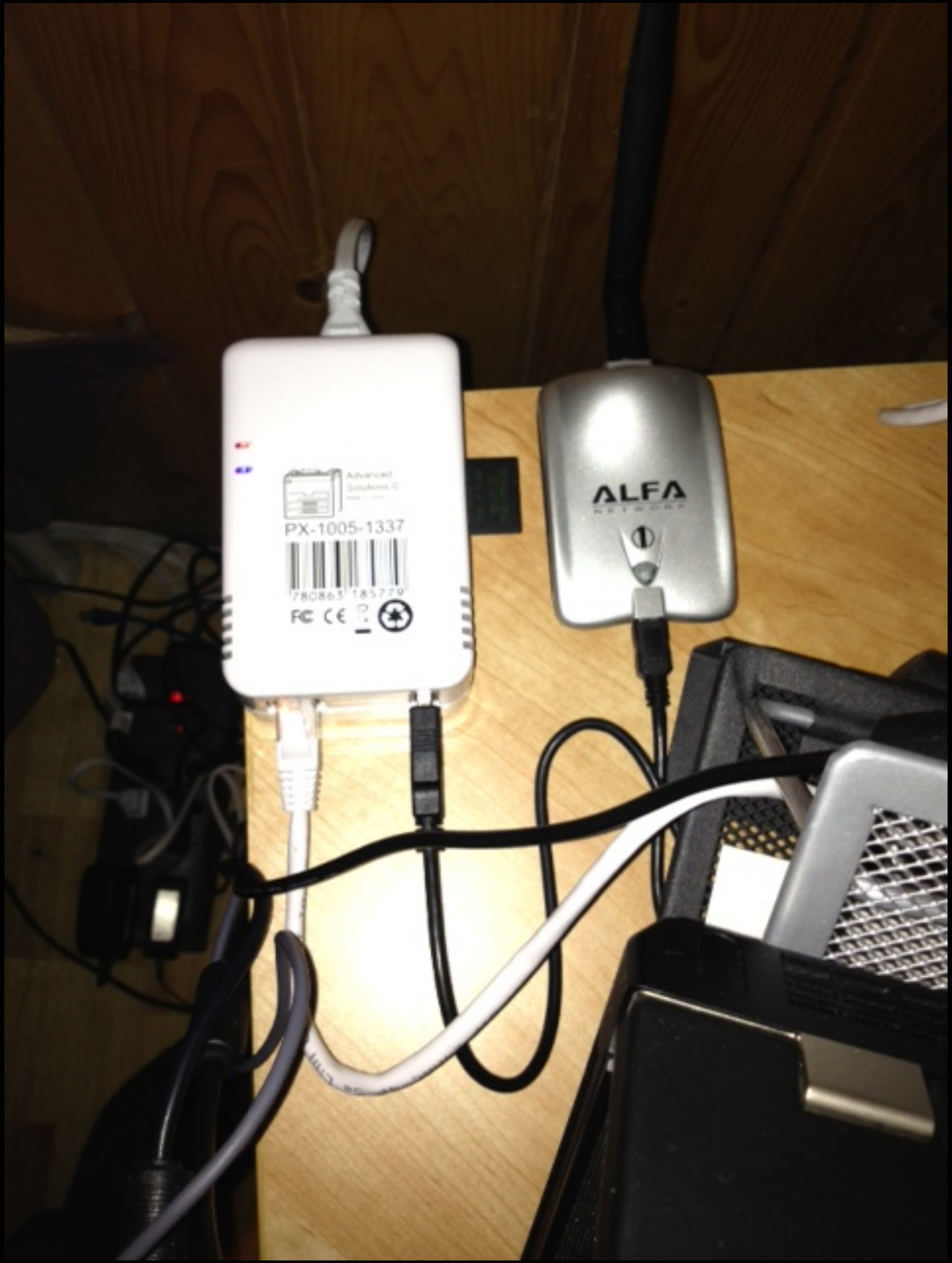
How can we use this information in a malicious ways?

- Unlocked Linksys PAP2 ATA + PwnPlug + Alfa Wireless USB wireless = PayPwn!
- Asterisk system() command lets us pass OS calls from DTMF
- Macro the most popular pentesting tools
- Cepstral/Festival TTS to receive responses

Nmap by Phone

Demo!

- PwnPlug has built in support for slimmed down Asterisk.
- Use Alfa to hook into a wireless network
- DTMF to initiate scans, cracking, etc etc


Advanced Solutions ©
PX-1005-1337
780863 185779
ALFA
NETWORK

There *are* easier ways to do this, but what the hell? This is fun.

Be honest with me. If you saw a Payphone, would you expect it to be a covert adventurer/badass?

Call Interception

Using the Asterisk ChanSpy() application we can monitor *all* voice traffic that goes through PBX.

Roll payphone into a Casino. Wait for people to use the phone. Listen. Magic.

Demo. Volunteer?

In summary

Using this information we can utilize Remote Telemetry to own any Elcotel Payphone

Like any archaeological dig, we can learn a lot about the way developers used to think

We can then apply this logic to other legacy systems still in the field (SCADA, etc)

PayPwn = Only limited by your imagination

If I have my way, they will live forever.

More information

- http://tinyurl.com/netwerked (Hack Canada Elcotel Archive)
- http://www.payphones.50megs.com/page7.html (some Elcotel docs)
- https://github.com/innismir/asterisk-scripts (nmap by phone)
- https://github.com/savantdc949/
- Payphone.com (thieving bastards)

Questions?

@savant42

http://dc949.org

Thanks!

- Defcon
- Tiffany and Gene Erik (for the payphone and code)
- docwho76 for the title image
- Hack Canada for the docs
- DC949
- Innismir, BlackRatchet, DaBeave, Strom Carlson, Binrev.com hackers, oldskoolphreak.com
- You!