```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 THE HIGH TECH HOODS and
 A-CORP PRESENTS.....

                 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
                 %%%                                %%%
                 %%%     THE ULTIMATE CELLULAR      %%%
                 %%%        PHONE PHREAKING         %%%
                 %%%        MANUAL #1 of 2.         %%%
                 %%%                                %%%
                 %%%          COMPILED BY           %%%
                 %%%           THE RAVEN            %%%
                 %%%                                %%%
                 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

(Sysops Note: None of this material COMPILED by Raven appears to be his own work! After examining some other files on cellular phreaking, I discovered some of the primary sources of his material are several articles written by The Mad Phone Man, an article on IMTS by The Researcher (of this bbs (P-80), and numerous other sources. Raven would suggest that this is his knowledge. One example of this a question and answer segment that Mad Phone Man had in one of his cell phreaking series. Raven has substituted his name where the answers are similar to a type writtin copy of a conversation, whereby the person speaking at the moments name is at the beginning of that line or lines. Thus it appears that Raven would like us to beleive him knowledgable on this subject. NOT! He has also removed all original credits of the real authors. Sounds like another teenager on an ego/power trip. However, even though some of this material is duplicated on this system, some is not, so im gonna run it. I do hope the technical data survived his COMPILING of this data better than his spelling and use of the english language.   Scan Man)

Hmmm.... Another text file.. Make sure that you keep this one for your collection!! There is no other text file that is more complete or up-to date that explains cellular phone phreaking like this one for 1992!!!

Since this is going to be a complete manual it has been broken-up into 2 parts so this is manual 1. I'm hoping that there will be some info. on cellular phreaking published in PHRACK that may be able to help you and me with our endevors but I'm waiting.

Another thing that I just found out is that the Hack/Phreak Community is in need for a BBS that doesn't give bullshit info (most do!) and thats cause our world has been infiltrated with narcs and telco/bell agents that try to spread as much misinformation as possible!! But there are a few bbs's that keep the faith and they will be listed at the end of this text.

THE RAVEN

+=======+

-=-=--=-=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=-=

INDEX....

=-==-=

CELLULAR PHREAKER TYPES

There are two types of cellular phone phreakers. The first type is the one whos's intrested in scanning cellular phone channels basically to overhear conversations. The second type is the one who obtains and modifies cellular equipment so that he can make free phone calls at someone elese's expense.

I. IMPROVED MOBILE TELEPHONE SERVICE

This system that was used prior to cellular phones was the Improved Mobile Telephone Service (IMTS), which was much easier to scan for.

Most scanner enthusiasts are familiar with this standard mobile phone system; this system has gone thru little evolution in the past decade in the U.S. It has remained a considerably limited service. A large metro area may only have several hundred users, (New York City has about 900 mobile phone subscribers) dur largely to limitations imposed by spectral overcroeding. Land mobile commo has seen a 10-12% annual growth rate for the past two decades. The result is that the 40, 150 and 450 MHZ bands are overcrowded. Even the utilization of the new 900 MHZ band (with 30-40 times more channels available than other bands) is a short-lived solution to the problem.

IMTS freqs (MHZ):

Channel	Base Freq.	Mobile Freq.
		VHF LOW BAND
ZO	35.26	43.26
ZF	35.30	43.30
ZH	35.34	43.34
ZA	35.42	43.32

ZY	35.46	43.46
ZR	35.50	43.50
ZB	35.54	43.54
ZW	35.62	43.62
ZL	35.66	43.66
	VHF HIGH-BAND	
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92
JS	152.69	157.95
YS	152.72	157.98
YA	152.75	158.01
JK	152.78	158.04
JA	152.81	158.07
	UHF BAND	
QC	454.375	459.375
QJ	454.40	459.40
QD	454.425	459.425
QA	454.45	459.45
QE	454.475	459.475
QP	454.50	459.50
QK	454.525	459.525
QB	454.55	459.55
QO	454.575	459.575
QA	454.60	459.60
QY	454.625	459.625
QF	454.650	459.650

The VHF high-band freqs. are the most popular IMTS channels. If you live within 25-50 miles of even a moderate sized town, you should have at least one VHF high-band channel. VHF low-band IMTS is used in rural areas and those with hilly terrain. UHF IMTS is primarily used in cities where the VHF channels are crowded. If you live in a major city, expect to have most, if not all, of these channels available to you.

II. GENERAL CELLULAR INFO

This section is a little boring but it's needed to set a basic foundation of cellular phone phreaking so that part 2 doesn't sound like all technicial talk!

The FCC originally estaablished 3 cellular bands. One was given to the local Bell or Telco, (wireline carrier), one to an independent firm (non-wireline carrier), and one reserved for future use. Originally there were 666 cellular freqs or channels. In recent years the FCC has tacked on another 156 freqs for a total of 832 freqs, and all cellular makers have upgraded their phones

to accomodate the new channels. Some of the new channels appears above the original 666 while others appear below.

The cellular system cannot know whether or not a cellular phone can be switched to one of the 156 channels without the phone telling it. This is done by the Station Class Mark (SCM), which is a 4-bit binary number.

(1) Bit #1 is "0" for 666 and "1" for 832
(2) Bit #2 is "0" for a mobile unit and
"1" for a voice activated transmit.
(That saves batteries on portables.)
(3) Bit #3 and #4 identify the power class
of the phone:
"00" = 3 watts
"01" = 1.2 watts
"10" = 0.6 watts
and "11" is not assigned.

The old traditional scheme for handling cellular traffic is the analog method or Frequency-Divison Multiple Access (FDMA). How the FDMA works is that free channels are found and each transmitter is assigned to one of them. When the call finishes, th echannels are freed up for the next call. Also, as the two parties become physically closer or more distant as they drive or travhghhggytel the call may be handed off to other freqs assigned to the new cells they are in.

Newer proposed schemes include Time-Divison Multiple Acess (TDMA) and Code-Divison Multiple Acess (CDMA). IN TDMA systems, calls may simultaneously use the same channels but are interspered between the pauses in the conversation. Many pauses result not only in the way people normally think and talk but when one party is talking, the other is listening. With TDMA, the Cellular Phone Company (CPC) injects small delays in parts of conversations to accommodate other traffic on that channel. This increases the lenght of the average phone call, which also increases their profits from it - not to mention the fact that they can increase there output by the factor of 3 and also then expand their operation.

CDMA is a system that's been used by military for the past 30+ years. CDMA appears to basically be a system where conversation are compressed into coded bundles and then decompressed at the other end.

A Cellular Mobile Telephone (CMT) is one that is installed in a vehicle, aircraft, watercraft or whatever, as opposed to a transporable or portable unit.

III. CELLULAR FREQS & CHANNELS

There are 832 cellular phone channels. 416 of these are allocated for the non-wireline services (Band A), and 416 for the wireline services (Band B). Each of these channels have two freqs, spaced 45 MHZ apart, that operate in a full-duplex mode. The lower freq is for the phone unit, while the upper is for the cell or basesite. Of the 416 channels, 21 are digital data control or "set up" channels and 395 are voice channels. Channels are numbered 1 thru

1023, and there is a gap from 800 to 990.

Rather than producing a list of 1646 cellular freqs, I have provided the math eqations that can be used to calculate them. These equations can be programmed into computers and calculators.

N = Cellular Channel # F = Cellular Freq
B = 0 (mobile), or B = 1 (base)

CELLULAR FREQS from CHANNEL #S:

F = 825.030 + B*45 + (N-1)*.03
WHERE: n = 1 to 799

F = 824.040 + b*45 + (N-1)*.03
where: N = 991 to 1023

CELLULAR CHANNEL #s from FREQS:

N = 1 + (F-825.030-B*45)/.03
Where: F > = 825.030 (mobile)
or F > = 870.030 (base)

N = 991 + (F-824.040-B*45)/.03
Where: F < = 825.000 (mobile)
or F < = 870.000 (base)

If the system uses OMNICELLS, as most do, you can readily find all the channels in a cell if you know just one of them, using tables constructed from these equations. Band A uses channels 1-333 under the old 666-channel system. To that have been added 667-716 and 991-1023 under the new 832-channel system. Band B uses channels from 334-666 under the old system, plus 717-799 under the new system.

IV. CONTROL & VOICE CHANNEL ALLOCATIONS

(D=DESIGNATOR, CC=CONTROL CHANNEL, VC=VOICE CHANNEL)

NON-WIRLELINE SERVICES (BAND A)

D = 1A : CC = 313 : VC = 1,22,43,64,85,106,127,148,169,190,211,232,253,274,
295,667,688,709,1003

D = 2A : CC = 314 : VC = 2,23,44,65,86,107,128,149,170,191,212,233,254,275
296,668,689,710,1004

D = 3A : CC = 315 : VC = 3,24,45,66,87,108,129,150,171,192,213,234,255,276
297,669,690,711,1005

D = 4A : CC = 316 : VC = 4,25,46,67,88,109,130,151,172,193,214,235,256,277
298,670,691,712,1006

D = 5A : CC = 317 : VC = 5,26,47,68,89,110,131,152,173,194,215,236,257,278
299,671,692,713,1007

D = 6A : CC = 318 : VC = 6,27,48,69,90,111,132,153,174,195,216,237,258,279
300,672,693,714,1008

D = 7A : CC = 319 : VC = 7,28,49,70,91,112,133,154,175,196,217,238,259,280
301,673,694,715,1009

D = 1B : CC = 320 : VC = 8,29,50,71,92,113,134,155,176,197,218,239,260,281
302,674,695,716,1010

D = 2B : CC = 321 : VC = 9,30,51,72,93,114,135,156,177,198,219,240,261,282
303,675,696,1011

D = 3B : CC = 322 : VC = 10,31,52,73,94,115,136,157,178,199,220,241,262,283
304,676,697,991,1012

D = 4B : CC = 323 : VC = 11,32,53,74,95,116,137,158,179,200,221,242,263,284
305,677,698,992,1013

D = 5B : CC = 324 : VC = 12,33,54,75,96,117,138,159,180,201,222,243,264,285
306,678,699,993,1014

D = 6B : CC = 325 : VC = 13,34,55,76,97,118,139,160,181,202,223,244,265,286
307,679,700,994,1015

D = 7B : CC = 326 : VC = 14,35,56,77,98,119,140,161,182,203,224,245,266,287
308,680,701,995,1016

D = 1C : CC = 327 : VC = 15,36,57,78,99,120,141,162,183,204,225,246,267,288
309,681,702,996,1017

D = 2C : CC = 328 : VC = 16,37,58,79,100,121,142,163,184,205,226,247,268,289
310,682,703,997,1018

D = 3C : CC = 329 : VC = 17,38,59,80,101,122,143,164,185,206,227,248,269,290
311,683,704,998,1019

D = 4C : CC = 330 : VC = 18,39,60,81,102,123,144,165,186,207,228,249,270,291
312,684,705,999,1020

D = 5C : CC = 331 : VC = 19,40,61,82,103,124,145,166,187,208,229,250,271,292
685,706,1000,1021

D = 6C : CC = 332 : VC = 20,41,62,83,104,125,146,167,188,209,230,251,272,293
686,707,1001,1002

D = 7C : CC = 333 : VC = 21,42,63,84,105,126,147,168,189,210,231,252,273,294
687,708,1002,1023

WIRELINE SERVICES (BAND B)

D = 1A : CC = 334 : VC = 355,376,397,418,439,460,481,502,523,544,565,586,607
628,649,720,741,762,783

D = 2A : CC = 335 : VC = 356,377,398,419,440,461,482,503,524,545,566,587,608
629,650,721,742,763,784

D = 3A : CC = 336 : VC = 357,378,399,420,441,462,483,504,525,546,567,588,609
630,651,722,743,764,785

D = 4A : CC = 337 : VC = 358,379,400,421,442,463,484,505,526,547,568,589,610
631,652,723,744,765,786

D = 5A : CC = 338 : VC = 359,380,401,422,443,464,485,506,527,548,569,590,611
632,653,724,745,766,787

D = 6A : CC = 339 : VC = 360,381,402,423,444,465,486,507,528,549,570,591,612
633,654,725,746,767,788

D = 7A : CC = 340 : VC = 361,382,403,424,445,466,487,508,529,550,571,592,613
634,655,726,747,768,789

D = 1B : CC = 341 : VC = 362,383,404,425,446,467,488,509,530,551,572,593,614
635,656,727,748,769,790

D = 2B : CC = 342 : VC = 363,384,405,426,447,468,489,510,531,552,573,594,615
636,657,728,749,770,791

D = 3B : CC = 343 : VC = 364,385,406,427,448,469,490,511,532,553,574,595,616
637,658,729,750,771,792

D = 4B : CC = 344 : VC = 365,386,407,428,449,470,491,512,533,554,575,596,617

638,659,730,751,772,793

D = 5B : CC = 345 : VC = 366,387,408,429,450,471,492,513,534,555,576,597,618
639,660,731,752,773,794

D = 6B : CC = 346 : VC = 367,388,409,430,451,472,493,514,535,556,577,598,619
640,661,732,753,774,795

D = 7B : CC = 347 : VC = 368,389,410,431,452,473,494,515,536,557,578,599,620
641,662,733,754,775,796

D = 1C : CC = 348 : VC = 369,390,411,432,453,474,495,515,537,558,579,600,621
642,663,734,755,776,797

D = 2C : CC = 349 : VC = 370,391,412,433,454,475,496,516,538,559,580,601,622
643,664,735,756,777,798

D = 3C : CC = 350 : VC = 371,392,413,434,455,476,497,517,539,560,581,602,623
644,665,736,757,778,799

D = 4C : CC = 351 : VC = 372,393,414,435,456,477,498,518,540,561,582,603,624
645,667,737,758,779

D = 5C : CC = 352 : VC = 373,394,415,436,457,478,499,519,541,562,583,604,625
646,668,738,759,780

D = 6C : CC = 353 : VC = 374,395,416,437,458,479,500,520,542,563,584,605,626
647,669,739,760,781

D = 7C : CC = 354 : VC = 375,396,417,438,459,480,501,522,543,564,585,606,627
648,719,740,761,782

To summarize how a cellular call is made: A mobile unit wishing to make a call will go off-hook and then transmit the digital source and destination codes on a control channel (used to set-up and monitor the call), and are just strong enough to reach the base station in the local cell. Upon getting this data, the base, thru its control freq (same channel), validates the mobile unit.

The base station then fowards a message to the central switching office on a land line, which in turn sends the paging signal to all cells in search of the second mobile unit whos number has been dialed. When the destination unit is finally found, it responds to the paging signal by transmitting an acknowledgement code to its local base station on a control channel.

The switching center then assigns a pair of unused freqs (called the, "channel Pair") to each of the unit for actual voice commo to take place. These channel pairs are not neccesarily the same for the respective cells that each mobile unit is in. These freqs are also relayed thru the base stations and to the central switching office.

When a unit moves into another cell, things get very interesting. Upon entry into another cell, the mobile unit must transmit thru a new base station. An automatic handoff to the new base station is carried out by another exchange of data thru the control channel.

Termination of the call is a simple matter. When the call ends,ON-hook signals are exchanged via the control channels between the mobile unit and the base station. The voice channels are then cleared.

IV. THE CELL & IT'S STRUCTURE

The cellular phone system uses a "honeycombed" hexagonal cell architure. Each of the cell types (A-G) differ from each other only in the freqs. allocated for them. This represents how a cellular system might be laid out. Cells A and B never share a common border. Neither do B and C, A and G, etc. Cells that are next to each other are never assigned adjacent freqs. They always differbu\y at least 60 KHZ. To track a mobile phone as it changes cells, lets put the mobile in a B cell. When the mobile switches freqs. you know that it could only go to a D, E, F, or G cell because A and C have adjacent freqs. The two tables below will help you determine which Channel cell can go next to each other. You can contact your local cellular phone company and see if they have any maps of the cell available in your area (please get a copy for us also). They're not obligated to give you maps but it's worth the try.

ADJACENT CELLS

Cell	Adjacent cells
A	C,D,E,F
B	D,E,F,G
C	E,F,G,A
D	F,G,A,B
E	G,A,B,C
F	A,B,C,D
G	B,C,D,E

The only fundamental point of cellular technology actually agreed upon to date is that a given service area will be divided into identical adjacent cells with no overlaps and no gaps. The hexagon is the standard cell patteren. At the center of an individual cell is a base station which is conected via land line to a local mobile phone switching office. Certain freq bands are assigned to certain cells, but not shared with adjacent cells to avoid mutual interference.

In 1979, AT&T began test marketing its version of a cellular phone system in Chicago. This system is call the Advanced Mobile Phone System (AMPS)

Some 2100 sq miles of the metro Chicago area are divided into 10 cells to serve about 2000 customers. Full duplex is possible by using a pair of one way channels separated by 45 MHZ to connect the mobile units with the base

stations. The RF range is 825-890 MHZ and normal narrow band FM is used to transmit voice. Hand-off to adjacent cells is accomplished by monitoring signal strengths. When the central switching office determines that a new base station receives the mobile signal better than the previous one, the switching office signals thru the voice channel for the mobile phone to switch to a new channel. Commo distruption thru the switching process is typically 50 milliseconds.

As with IMTS, there is the possibility of phreaking calls with IMTS or AMPS simply by monitoring the control channels since they are in dial pulse form. After you have a nice set of numbers, you will neeed a transmitter of sufficient strenght to reach the base station (unlicenced transmitter of course!). Duhh

Many regulatory and implementation issues remain unsolved. Modulation issues are the biggest problem to be solved. Single sideband AM, narrow band FM, digital and spread-spectrum techniques are all being considered. If you have any info that may be able to break this down for fellow hackers/phreaks please leave me mail.

V. EQUIPMENT DESCRIPTION

Most mobile phones have two primary pieces of equipment. These are the transceiver (transmitter-receiver pair) and the control head.

The transceiver is usually a metal box with three connectors. They usually contain two circuit boards. One is the transceiver unit itself, and the other is a logic board consisting of a uP, ADC and DAC, and control logic. The transceiver is usually mounted in the trunk or sometimes under the hood, and is connected to both the ignition switch and car battery. A control/audio (shielded) links the equipment together.

The control head is a touch-tone phone handset with the extended keypad, alphanumeric display and controls (i.e. mike, volume). Usually there is a separate speaker installed in the cradle for on-hook dialing, call progress monitoring and speakerphone operation. If the CMT has a speaker phone option a small mike is usually mounted to the sun visor. Some cellular phones are voice-activated. If battery-operated, this saves the battery and also makes answering the phone easier. The control head and cradle assembly is usually bolted to the hump between the two front seats for security purposes.

Most early CMT's use the AMPS bus (developed by AT&T) which uses a system of 36 wires in a rather bulky and stiff control/audio cable. Some makers now use their own bus, such as Novatel's serial bus, which specifies a thin cable consisting of a few wires, and is much easier to install and dependable to use. In almost all cases, a CMT is powered by regulated 12 volts from standard 13.8 volt car battery. At least 5 amps (continuous) is required.

Mobile cellular antennas are usually short (less than one foot long), vertically-mounted stiff wire with a few turns in the middle that acts as a phasing coil in a 5/8-wave configuration. The antenna is generally mounted either thru a hole in the roof or at the top of the rear winshield using silicone rubber cement with conductive plates on both sides to pass the RF thru the glass (some RF losses result from this method but you don't have to

maim your vehcle). A 50 ohm coax cable (ex: RG-58/U) links the antenna to the transceiver with a male TNC type UHF connector. A ceramic duplexer permits the transmitter and receiver to share the same antennas at the same time.

CMT roof-mounted monopole antennas are designed to work with the ground plane (ie: the vehicle's body, if metal). However, for fixed (ie: home-base) use, an "extended-feed" or voltage-fed coaxial antenna (requires no ground plane) can be used. A capped PVC pipe makes an ideal rooftop housing for this type of antenna-both weatherprofing and concealing it. Note that altho cellular systems are designed for inefficient antennas, for fixed use it is preferred that you use the best antenna you can get.

Interfacing audio devices (ex Blue Boxes, other tone generators) to a CMT can be done by coupling the device's output thru an audio coupling transformer wired across the control head's mike lines. A 600-ohm audio coupling antenna is availble from Radio Shack (273-1374). Be sure to DC isolate the phon circuity by wiring the transformer in series with a non-polarized capacitor of at least 1.0 uF and 50 volts. If you can locate the bus that carries the audio, then coupling across it is preferred.

An acoustic modem can be coupled to a CMT eithrer thru the mouthpiece or by connecting the mike and speaker wires to those in the control head or bus lines. Any direct-connect devices (ex: answering machines, modems, standard phones, etc) can be connected to a CMT thru the AB1X cellular interface made by : Morrison & Dempsey (818 993-0195). This expensive device is basically a 1-line PBX that connects between the transceiver and control head and provides an RJ-11C (quick-connect) jack that accepts any direct-connect phone accessory. It recognizes both touch-tone and pulse dialing, provides the ringing voltage and generates dial and busy tones as needed.

VI. GENERAL PHREAKING INFO

Some Definitions:

* Control Channel: The channel the phone and cell base first communicate on.
* Reverse Control Channel: The opposite freq, 45MHZ lower then the control channel. This is where the mobile unit is.
* Voice Channel: The channel you are assigned by the switch to start the call after the exchange of suscriber data.
* Revese Voice Channel: Again 45 MHZ lower.
* Switch: The computer that places the calls, and takes and receiver data from the subcriber or from the PSTN. (Pubic Swithced Telephone Network). That should get things started. A suscriber picks up his handset to place a call.

QUESTIONS AND ANSWERS

The following questions & answers were taken from THE SOURCE BBS a.k.a. THE NEW YORK HACK EXCHANGE

BCOM> I want to get into cellular phone phreaking but I dont know anything so I'm depending on you guys to help me out from the VERY basics! What is cellular; a cellular phone?
RAVEN> A 800 MHZ radiotelephone, running 3 watts, with the ability to change channel on computer command from the central swith. This happens when you travel thru the service area and your signal becomes stronger at a neighboring cell base station.

BCOM> They are marketed as a high security device with no possibility of anyone making a phoney call & charging it to someone else, how can it be phreaked?
RAVEN> An understanding of the phone revels that every time a call is made, the phone number, an electronic serial number, and oother data is sent to the switch. If you were to listen to the opposite side of the control channel as the cell is being "set up" you would hear this data being transmitted to the switdch in NRZ (Non-Return to Zero) code. All one has to do, is record this info and program the bogus phone to these params, and then a free call is possible thru the switch.

BCOM> Has anyone done this yet?
RAVEN> HELL YEA! about 6 months after the first cellular phone system was "turned-up", a technician programmed a Panasonic telephone with a NEC ESN (Electronic Serial Number). And there have been many other cases since then. With the popular ROM programmers avaible today, almost any NAM (NUmeric Assignment Module) can be duplicated or copied with changes. (The NAM is the heart of the billing info and contains the phone number but not the ESN) The most popular integrated circut for NAMs is the 74LS123.

BCOM> Sounds like a lot of trouble, is there easier ways to get service?
RAVEN> SURE, the cellphone companies have been their own downfall, In an effort to market their wares as a universal service. Nobody can tell if a phone from another city (that has a roaming agreement) is valid until its too late. The only thing they could do after finding out is block any call with bad ESN because as we know, the phone number is easy to change, but the ESN is not.

So here's a likely scenario====> A roamer identifying itself as a number from a Chicago non-wireline accesses a cellular system in Dallas. An operator may intervene but you can usually BS or "Social Engineer" them as long as you know the data you have programmed into your phone. Then you make calls just like your a local user. If your found out, you change the number to another, and see if that works.

The phone is locked onto the strongest control channel in the area by a computerized scanner in the phone. As the user drives thru the service, a computer constantly picks out the strongest control channel and stays on it,

altho more than one cell site can actually be herd. The subcriber enters the number to call on the keypad, and presses the "send" button.

At this time the following data is transmitted to the cell site by the mobile. The callers ESN, his home system number (two digits), his mobile's area code and phone number, and the called number. The cellular switch now picks up an outgoing line, places the call for him and tells the mobile unit to switch to a voice channel. The two ends are linked in the central switch and the two parties are connected up in about 3 seconds.

I have purposely over-simplified the whole process to point out the moment of truth. The mobile's ESN and phone number and data in the switch must match or no go. This is required for billing purposes. If one had the ESN and the mobile phone number, he could then calll anytime anyplace without fear of a trace - let alone a bill. The ideal setup would let you listen to the reverse control channel, record and display herd working numbers and ESN's, and recall them as one needs them to make calls.

This would be it but we are not quite there yet. But some hard work has already been done for us. All the aforementioned codes are sent in hex, in NRZ code (phancy term for phase shift keying), but the phone already has, for example, a NRZ receiver and transmitter built right into it. All that has to be done is to have a receiver on the reverse control channel, recover the other users data and save it or at least print it out.

The mobile radio data book show some good technical info on the systems used and chip part numbers for the NRZ stuff. For example, at least one cellular phone maker uses the 8085 chip for the control head functions - a popular and well understood chip by many.

Most cellular phones include a crude password system to keep unauthorized users from using the phone - however, dealers often set the password (usually a 3 to 5 digit code) to the last four digits of the mobile phone or there home phone. If you can find it somewhere on the phone then your in luck!! If you can't find it then I guess you gotta hack it. It souldn't be that hard since most people aren't smart enogh to use something besides "11111", "12345", or whatever, it will be like Hacking a VMB.

If you want to modify the chip set in the cellular phoneyou got, there are two chips (of course this depends on the model and maker - your may be different) that will need to be changed - one installed by the maker usually eepoxied in with the phone's ID number, and one installed by the dealer with the phone number, and possible the security code. To do this youll obviously need an EPROM (Erasable Programmable Read-Only Memory) burner, as well as the same type of chips used in the phone (or a friendly & unscruplus dealer!).

As to recording the numbers of other mobile phone customers and using them; as far as I know it is quite possible, if you got the equipment to record and decode it. The cellular system would possibly freak out if two phones (with valid ID/phone number combinations) were both present in the network at once, but it remains to be seen what will happen.

The MIN is the Mobile Identification Number (includes the phone number, and it is stored on the NAM ROM). Stolen and spoofed ESN's and MINs are good for about a month. Once a bad MIN is revealed, the legit user's MIN is changed by the Mobile Telephone Switching Office (MTSO) and they arrange for a new

NAM ROM to be installed in the users legit unit. Of course MTSO keeps a database of all legit,illegit and deadbeat MIN/ESN pairs. However, the MTSO will allow a illegit MIN/ESN pair to continue to function beyond its discovery in hopes of discovering who the phreaks are.

One of the properties of cellular phone system is that the transmitter freqs may be changed or "hopped" in the constant effort to allocate freqs. Because of freq. hopping it is very difficult triangulate a CMT using standard RF directional finding methods. It is known that a directional antenna randomly aimed at cellsite repeaters will confuse directional finding equipment being used by them that is synced to their freq. hopping scheme.

ROAMING

Since cellular technology often results in physical seperation between the caller and-or callled party from landlines, because it offers thousands of lines to choose from, because freq. hopping occurs, and because the caller and-or called party can be rapidly moving from one location to another, cellular phnes are the safest form of phreaking. "Roaming" is one form of cellular phreaking.

Roaming occurs when a CMT is used in a cellular system other than the one indicated in the NAMs SID. This is called "ROAMmode", and the ROAM indicator on the control head will light. A CMT can roam into any system its home CPC has a roaming agreement with, and most CPC's now have roam agreements with each other. Not every system pays attention to a "Roamer" from outside the system as cosely as they do a local suscriber. In their mad rush to offer cellular as "universal" service, they screwed up. If there's no roam agreement, the MTSO will transmit a recorded message to the CMT with some instructions to call the CPC, and gives his name ,MIN,ESN and credit card number. All roamed calls will then be completed by the MTSO and billed to the credit card account. This procedure is becomming less common as more roam agreements are made.

Usually, CPC can only determine if a roamer came from a system with which it has a roaming agreement - nit the creditworthiness of the roamer. Consequently, many CPCs have been ripped-off by roamers who've been denied service on their home system because they are deadbeats. Once the home CPC is billed for the roaming services provided by the remote CPC to the phreaker or deadbeat, it will notify the same to add that ESN/MIN pair to their MTSO's "negative verify" file to prevent future abuses.

Several independent firms are establishing systems software and data networks to allow POSITIVE ROAMER VERIFICATION (PRV), which allow near real time roamer validation bt sharing data between CPCs. Until PRV becomes universal, even bogus ESNs and MINs can roam if they follow the standard format, alto some CPCs are sharing roam data on a limited basis to prevent this. Even with PRV, ESN/MIN pairs that are spoofed to match valid accounts will be accepted both by thier home CPC and roamed CPCs, until the legit customer complains about the calls he didn't make. And even without PRV, some CPCs automatically share ESN and MIN data. This frequently occurs between the CPCs in major cities and those in their bedroom communities.

To call a roaming CMT, the caller must know which system that unit is in, which can be a real trick since he may be on the road at the time. He then calls the CPC's roaming number. Roaming numbers vary but usually are in the phone number format (with area code, with the last four digits being "ROAM", and with the 3 middle digits being the remote CPC's exchange). When that number is called, a dial or ready tone is returned, after which the roaming CMT's full MIN is entered in Touch-Tone. After several seconds, the CMT will ring or the caller will hear a recording stating that the roaming CMT is out of range or busy. Telocator Publications (202) 467-4770 publishes a nationwide roaming directory for travellers with celluar phones.

For example: I access the Cleveland Ohio Cellular 1's Ericcson switch and I tell them by my NAM INfo that I'm a roamer from NYNEX in New York City. Cleveland will let me make the call, bacause it bills back to NYC for the number of minutes I use. If the NYC number is bogus , the call goes thru anyway, and the bill doesn't go anywhere. They do know the exchange data for NYC (that's on a chart) so you can't tell them a wrong system number (two digits) but one that a valid roamer would have from his area. This is not too hard to figure out, call some of their stupid sales idiots some time and see what they let out of the bag.

The system number for the foreign exchange, NYNEX in Buffalo is 56, Chicago nonwireline is 01, and Buffalo nonwireline is 03. All wirelines are even numbers and all nonwirelines are odd. The first three digits of the mobile number: NYNEX Buffalo 863-XXXX. Buffalo Non-wirelines are 861-XXXX and 690-XXXX.

You dont have to be a rocket scientist to figure out the local numbers for your area, again by conning the sales people. Until the CPC's get a cellular clearinghouse to validate roamers in real time, this method will work out fine. It will be awhile before it becomes routine to look up a roamer. There's simply to many to look up every time service is wanted. And this problem is increasing because of the expanding use of cellular phones.

If a cellular phone and its antenna happen to fall into your hands, you could re-nam it as a roamer and when you get it setup, make copies of the info with different suscriber numbers (the last 4 digits) and make free calls as long as you can.

THe Novatel series phone a re probaly the best radios to use to shut down a cell site completely as it has secret codes in the control head that allow you to bypass conventional switching protocols.

NOTE

I hope that this file has lived up the all the boasting I've put into it. But if there are any problems with the freqs. or anything you can leave me mail on the bbs's I've listed. At this time Demon Roach and Nihilism dont carry my files but you can still leave me mail on those boards!

THE RAVEN

+=======+

=-=

Thats it for part 1 but look out for part 2!!

Part 2 will cover: What's in a NAM, NAM reprogramming and how to reprogram the following phones: DIAMONDTEL MESA90X & MESA99X HANDHELD, GATEWAY CP 900 HANDHELD, GENERAL ELECTRIC MINI II & MINI , MITSUBISHI 800 & 900 , MOTOROLA 8000H & ULTRA CLASSIC HANDHELD, NEC P300 & NEC P9100 , NOVATEL PTR800 & 825 , OKI HANDHELD MODEL #750, OKI HANDHELD MODEL #900 , PANASONIC EB3500 , COLT TRANSPORTABLE , DIAMONDTEL MESA 55 & MESA 95 TRANSPORTABLE , FUJITSU MOBILE PHONE , GENERAL ELECTRIC CARFONE XR3000 , GOLDSTAR SERIES 5000 MOBILE , MITSUBUSHI 555,560,600 , NEC M3700 SERIES MOBILE , NOKIA LX-11 & M-10 , NOVATEL 8305 TRANSPORTABLE CA08 SOFTWARE VERSION , OKI CDL400 , PANASONIC EB362 , PANASONIC EB500 OR TP-500 , RADIO SHACK 17-1002 & -1003 , AND GE CARFONE MODELS CF-1000, CF-2000 & CF-2500

So look for it at a BBS near you!!

THE RAVEN

+=======+

^^^