

CELL1.TXT

CELLULAR TELEPHONE PHREAKING PHILE SERIES VOL 1 by The Mad Phone-man

How would ya like to have a phone that no body could locate? How bout free phone service on it too? Well Cellular telephones have the potential to do all this and more. First lets discuss some basics of the service.

Q:What is cellular a cellular phone?

A: A 800 mhz radiotelephone, running 3 watts, with the ability to change channel on computer command from the central switch. This happens when you travel thru the service area and your signal becomes stronger at a neighboring cell base station.

Q: They are marketed as a high security device with no possibility of anyone making a phoney call and charging it to someone else, how can it be phreaked?

A: An understanding of the phone reveals that every time a call is made, the phone number,an electronic serial number, and other data is sent to the switch. If you were to listen to the oposite side of the control channel as the call is being "set-up" you would hear this data being transmitted to the switch in NRZ code (non-return to zero). All one has to do, is record this info and program the bogus phone to these params and a free call is possible thru the switch.

Q: Has anyone done this yet?

A: YES, about 6 months after the first cellular phone system was "turned-up" a technician programmed a panasonic telephone with a NEC E.S.N. (Electronic serial number) this was reportedly done for a gram of coke. With the popular ROM programmers available today, almost any NAM (Numeric Assignment Module) can be duplicated or copied with changes. (The NAM is the heart of the billing information and contains the phone number but not the ESN) The most popular integrated circuit for NAMs is the 74LS123.

Q: This sounds like a lot of trouble, is there easier ways to get service?

A: SURE, the cellphone companies have been their own downfall. In an effort market their wares as universal service (Your phone will work in any system) they have let the cart get before the horse. Nobody can tell if a phone from another city (that has a roaming agreement) is valid till its too late. The only thing they could do after finding out is block any call with the bad ESN because as we know, the phone number is easy to change, but the ESN is not. So heres a likely plot...a roamer identifying itself as a number from Chicago non-wireline accesses a Cellular system in Dallas. Sometimes an operator intervienes but you can bullshit them as long as you know the information you have programmed into your phone. Then you make calls just like you are a local user. If you're found out, you remove the number, change it to another, and see if that works. Usualy it will require the radio's ESN chip to be changed, but thats a lot easier if you have a ZIF (zero insertion force) socket installed, thats what I use.

Upcomming soon, more good info on particular mfgrs ESN codes.
Cracking the Motorola switch, Shortcommings of the Ericcson AXE-10 switch.

>>> The Mad Phone-man <<<

CELL1.TXT

Downloaded From P-80 International Information Systems 304-744-2253