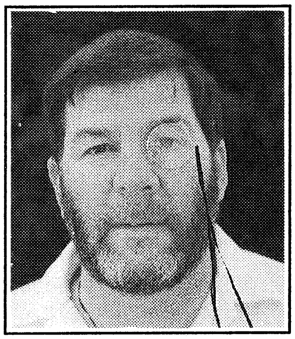
Moffat's Madhouse...

by TOM MOFFAT



The Phone Phreak Phenomenon

I have recently been reading a book called *Cyberpunk*. It is the definitive history of computer hacking, back in the days when it was considered a reputable sport (well, almost), instead of the vandalism it's thought of today. Hackers with names such as Pengo and RTM spent their leisure hours trying to penetrate the early computer networks, generally with a view to simply 'entering' a distant computer system. They weren't there to do harm, just 'enter', and possibly leave behind a calling card to prove that they had done so.

Much of this activity centred on prestigious universities such as Cornell and Dartmouth, in the northeastern United States. These universities ran innovative computer science faculties which encouraged learning by experiment, as well as by direct instruction. A badge of honour among students was to do something with a computer that had never been done before. This was known as 'hacking', and it went on with official sanction. Many a Master's thesis and Doctoral dissertation came about as a result of some creative hacking.

The people who became hacking legends did so by spreading their wings beyond the bounds of the university's computers, moving across the networks and into machines on the other side of the world. Unfortunately people like Pengo and RTM, once inside the remote machines, couldn't resist nicking the occasional bit of software or a military secret. They went to jail, their names were mud, and hacking became a Bad Word.

But the 'good' meaning of hacking still persists to this very day; it is given to something that is done in a new and remarkably simple way, breaking all the established rules. I must admit I was very flattered when one of my projects, the Wesat weather satellite decoder, was described as a 'neat hack' because of the way it decodes the signal without using a demodulator.

The Internet is the world's largest computer network, and the one that landed RTM in jail when his experiments to penetrate Internet computers went wrong. And on the Internet to this very day there are file areas labelled 'hacks', where you can expect to find the most innovative and unusual software.

Unfortunately my university days were a bit too early for hacking. Computer Science courses did not exist; in fact computers barely existed, and those that did were multi-million dollar mainframes attended by people who were basically mathematicians. Nobody had thought of tying computers together with networks, so there was really nothing to hack. That's a pity, because I probably would have been in it. Well, maybe in jail too. I suppose it's better there weren't networks....

Ah, but there were! They were called 'long-distance telephone networks' and they let people all over the country talk with each other. It was customary to pay a fee for this privilege, but early 'hackers' devoted much time and energy into avoiding the necessity to pay for long distance phone calls. This, as with computer hacking, was more for the sport than for financial gain. People who took part in this interesting activity were known as Phone Phreaks. Pengo and RTM started their hacking careers as Phone Phreaks. And I was certainly around during the Phone Phreak era — strictly as an observer, you understand...

The 'crony bar'

The first Phone Phreak device was not electronic at all, but a piece of coat hanger wire. This wire, known as a 'crony bar', had a small handle looped into one end, followed by a 90° bend to the left, and then a 90° bend straight up. The device was inserted into the coin return chute of a pay phone, and when jiggled correctly it would make coins inserted at the top come straight out through the bottom.

The crony bar, as I remember, was developed by students at the above-mentioned Dartmouth University. (Later on, they produced the BASIC computer language.) And, if memory serves me rightly, construction details were published in a magazine, which I think might have been *Playboy*. Crony bars were a boon to impoverished university students who needed to call home for more money.

Eventually the American Telephone Company had to develop a whole new model of pay phone, which was immune to the crony bar. These phones had a little pull-down gate on the coin return, which blocked the passage up into the phone when the gate was opened, preventing the entry of crony bars.

Infamous 'Blue Box'

With the demise of the crony bar a new line of attack was needed, and this time it was provided by electronics, via a gadget known as the 'Blue Box'. The Blue Box didn't just work on pay phones; it could force nearly any phone in the land to make free trunk calls, dialled up on an early 'numeric keypad' on the front of the box. I remember once seeing a photo of a Blue Box in a magazine — and sure enough, it was blue.

The Blue Box was publicised, but construction details were not. These were kept as 'secrets of the clan' by practicing Phone Phreaks; after all, they had to have something that made them stand out from the general public. But with a bit of knowledge of how the phone network operated back then, it wasn't hard to surmise how a Blue Box worked. Experiments proved the theory correct, and opened the way for a new Blue Box that didn't need any special electronics at all — only a tape recorder.

So now, 30 years too late, we now present full technical details of the Blue Box; enough information for you to build one for yourself. However you needn't bother, because it won't work on the Australian phone network. It appears the system isn't sensitive to the crucial 2600Hz 'SF' tone.

The American phone network, in the sixties at least, depended upon Dual Tone Multi-Frequency (DTMF) tones to dial numbers through the trunk network. These circuits could handle only audio, not DC, so dial pulses had to be converted to tones. The same went for on-hook/off-hook information. This was transmitted as 'signal frequency' or SF.

Around this time, DTMF dialling was becoming popular in home phones as well; everyone wanted a push-button phone with 'Touch Tone'. These are all the rage nowadays too, and in Australia we are familiar with the sound of the beep-boops as we push the buttons on one of these phones. But in America, Touch Tone phones were incapable of dialling along the trunk network because the trunks used *different* tones, and these were supposed to be a closely-guarded secret.

'Secret' tones

When a subscriber wanted to dial a long-distance call he would punch in the number on his Touch Tone pad or rotary dial, and these tones or pulses were decoded and then re-transmitted along the trunks as 'secret' tones by equipment within the exchange. This process was supposed to be unknown to the subscriber, but many times you could hear a quick burst of new DTMF tones being shot along the network to the other end.

The 'secret' tones, however, soon became known. One source was the Howard Sams book *Reference Data For Radio Engineers*, where the scheme is detailed on page 2-13. For various operational reasons it is necessary to send numbers of varying lengths along trunk circuits, so the 'secret' scheme contains some extra signals: A 'KP' tone burst tells the system that some digits are to follow, and an 'ST' burst signals when they are finished.

Other tones signify the digits 1-10. Each signal is made up of a pair of frequencies, as described below:

Digit	Frequencies (Hz)
KP	1100 + 1700
1	700 + 900
2	700 + 1100
3	900 + 1100
4	700 + 1300
5	900 + 1300
6	1100 + 1300
7	700 + 1500
8	900 + 1500
9	1100 + 1500
0	1300 + 1500
ST	1500 + 1700

The only other tone to mention is the 'SF' signal-frequency tone, which is 2600Hz. The presence of SF means the circuit is 'on-hook', and its absence means 'off-hook'.

When dialling is to take place, the originating end kills the SF tone, telling the far end that its 'phone' is off-hook. The far end responds with a high-level blip of SF, called a 'sender', and then continues sending normal-level SF as the number is dialled. If the far end answers, it is off-hook and the SF from there is killed. Then there are no tones on the circuit, and a conversation can take place.

The most interesting feature of this, from a Phone Phreaking point of view, is that either end can force the other end to hang up by hitting it with a blast of SF tone. This of course happens when either party hangs up (goes on-hook). But you can also cause the far end to go on-hook, without you yourself actually hanging up, by playing a 2600Hz SF tone into your telephone's mouthpiece. This is the Phirst step of a Phone Phreak session...

Upon hearing the SF, the far end goes on-hook. But if you now kill your SF again, the far end responds with a new 'sender', and it is ready to receive another number. Now you put your Blue Box up near the mouthpiece, punch KP, punch in the number, and then punch ST. Your new call is away! But your phone is still physically 'off the hook', and the exchange thinks you are still connected with your original call.

Of course it is necessary to get into the trunk network in the first place for Phone Phreaking to work, but this is simply a matter of making a trunk call. For this, of course, you will be charged. But there are such things as FREE trunk calls, like when you ring the time and the talking clock is physically in a different city. You can stay on the talking clock as long as you like for the price of a local call, making one Phone Phreak call after another.

One can avoid the necessity of a proper Blue Box by using two audio oscillators and a reel-to-reel tape recorder. You simply set up the oscillators to produce the correct two tones, combine them through a simple resistive divider, and record two or three minutes of each tone combination.

Before making a call you must get your scissors and sticky-tape and edit together the correct sequence of SF, KP, the numbers, and ST, and then play the resulting tape into the telephone.

This sounds like an awful lot of trouble, but it produces the desired effect. You succeed in beating the system. The biggest problem for Phone Phreaks is trying to think of someone to ring. Once you've cracked the network all the fun is gone out of it.

Many Phone Phreaks demonstrate their skills by ringing distant recorded services; for instance 617-536-4050 gives you (or used to give you) a recording of the activities of the bird watching society in Boston. In New York you could try 212-759-1520 to get a recording from a bedding shop, designed to put you to sleep. In San Francisco, 415-LOSTDOG gave a list of — you guessed it! Really keen Phone Phreaks rang the White House, or the Kremlin.

It's very doubtful any of this stuff still works, although one never knows in the USA where the telephone company has been known to squeeze 40 years life out of a piece of central office equipment. As I mentioned earlier, it does NOT work in Australia, and you may well bring down the wrath of Telecom upon your shoulders should you get caught squirting strange tones down the line.

In the USA, Phone Phreaks face new challenges from the computer technology taking over the phone network. I have read that Ma Bell over there has even developed Phone Phreak detectors, which can pinpoint any new Blue Box designs and send the cops running.

Despite the dangers, or perhaps because of them, I see from things I've picked up on computer bulletin boards that Phone Phreaking is still alive and well in the USA. But now, like so many other activities, it's a crime that can send you to prison and screw up your life good and proper. Best avoid it now, I guess. Get yourself a copy of *Cyberpunk* instead. ❖