File: A HISTORY OF BRITISH PHREAKING
$$ $
$ $ The History Of British Phreaking $
$ -=- -=-=-=- -- -=-=-=- -=-=-=-=- $ $
$ $ The second in a series of $
$ THE HISTORY OF.....philes $ $
$ $ Written and Uploaded by: $ $
$ $$$$$$$$$$$$-=>Lex
Luthor<=-$$$$$$$$$$$ $ and $
$ The Legion Of Doom! $
$$With thanks to Peter McIvers for the list of frequencies mentioned later inthis phile.NOTE: the British Post Office, is the U.S. equivelent of Ma Bell. In Britain, phreaking goes back to the early fifties, when the technique of 'Toll A drop back' was discovered. Toll A was an exchange near St. Pauls which routed calls between London and nearby non-London exchanges. The trick was to
dial an unallocated number, and then depress the reciever-rest for 1/2 second. This flashing initiated the 'clear forward' signal, leaving the caller with an open line into the Toll A exchange. He could thjen dial 018, which forwarded him to the trunk exchange- at that time, the first long distance exchange in Britain- and foll ow it with the code for the distant exchange to which he would be connect ed at no extra charge. The signals needed to control the UK network today were published in the"Institution of Post Office Engineers Journal" and reprinted in the Sunday Times (15 Oct. 1972). The signalling system they use: signalling system No. 3 uses pairs offrequencies selected from 6 tones separated by 120Hz. With that info, thephreaks made "Bleepers" or as they are called here in the U.S. "Blue Box", butthey do utilize different MF tones then the U.S., thus, your U.S. blue box thatyou smuggled into the UK will not work, unless you change the frequencies. In the early seventies, a simpler system based on different numbers of pulses with the same frequency (2280Hz) was used. For more info on that, try toget ahold of: Atkinson's "Telephony and Systems Technology". The following are timing and the frequencies for boxing in the UK and other foreign countries. Special thanks to Peter McIvers for the phollowing inpho:British "bleeper" boxes have the vaery same layout as U.S. blue boxes. The frequencies are different, though. They use two sets of frequencies, forward and backward. Forward signals are sent out by the bleeper box; the backward signals may be ignored (it's sort of like using full duplex). The frequencies are as follows:U.S.:US: 700 900 1100 1300 1500 1700Forward: 1380 1500 1620 1740 1860 1980 HzBackward: 1140 1020 900 780 660 540 Hzfor example, change the 900 Hz potentiometers in your box to 1500 Hz. All numbers 1-0 (10) are in the same order as in an American box. The ones after this are thier codes for operator 11, operator 12, spare 13, spare 14, and 15. One of these is KP, one (probably 15) is Star; it won't be too hard to figure out. The signals should carry -11.5dBm +/- 1dB onto the line; the frequencies should be within +/- 4Hz (as is the British equipment). Also, the 1VF system isstill in operation in parts of the U.K. This would encode all signals 1 to 16 as binary numbers; for instance, a five is 0101. There are six intervals per digit, each 50ms long r a total of 300ms. First is a start pulse of 2280 for 50ms.

Then, using the example of five (0101), there is a 50ms pause, a 50ms pulse of 2280, a 50ms pause, and a 50ms pulse of 2280. Finally, there is a 50ms pause that signals the end of the digit. The frequency tolerance on the 2280 Hz is +/- 0.3%; it is sent at -6 +/- 1dBm. An idle line is signaled by the presence of a 3825Hz tone for more than 650ms. This must be within 4Hz.France uses the same box codes as the US, with an additional 1900Hz acknowledgement signal, at -8.7 +/- 1dBm per frequency.Spain uses a 2 out of 5 mf code (same frequencies as US), with a 1700 Hz acknowledge signal.Other places using the 1VF system are:Australia, 2280Hz +/-6Hz, 35ms/digit at -6dB.Germany, France: same as Australia; also, some 1VF systems in the UK.Switzerland: same as Australia, only it uses 3000Hz, not 2280.Sweeden: same as above, but at 2400Hz.Spain: some parts use 1VF with 2500Hz.There is one other major system: the 2VF system. In this system, each digit is35ms long. The number is encoded in binary as with the 1VF system. Using the example of five (0101), here's how the American 2VF system was sent:2400 pulse, pause, 2040 pulse, pause, 2400 pulse, pause, 2040 pulse, pause. Thedigits and pauses are all 35ms long, for a total of 280ms per digit. Other countries are still using a similar high/low pair with the same timings. Some parts of Italy use the 1VF system with 2040Hz; some use the 2VF system with 2040 and 2400 (same as original US) Hz. The Netherlands uses a 2VF system with 2400 and 2500 Hz pulses. With the 2VF system, all frequencies should be within2Hz.Also, here are some specs for American phone equipment:Dial Tone: 350+440Hz, -17.5 to -14.5 dBm/tone.Off-Hook (ROH): 1400+2060+2450+2600(!) on/off 5 times per secondBusy: 480+620Hz; solow busy: 0.5 +/- 0.05 sec = 1 period(about twice a second), at -28.5 to -22.5 dBm/tone.Ring: 440+480 Hz at -23.5 to -20.5 dBm/tone.A ring is modulated at 20 +/- 3Hz, 2sec on, 4sec off.Call waiting: 440Hz, on 1 second.Recorder Connection: 1400Hz, beeps every 15minutes.Multiparty line ring: sam% frequency and modulation as ring, but 1sec on, 2sec off (twice as fast). Now, back to British Phreaking:In the early days of British phreaking, the Cambridge University Titan Computer was used to record and circulate numbers found by the exhaustive dialing of local networks. These number s were used to create a chain of links from local exchange to local exchange across the country, bypassing the trunk circuits. Because the internal routing codes in the UK network are not the same as those dialed by the caller, the phreaks had to discover them by 'probe and listen' techniques or more commonly known in theU.S.--SCANNING. What they did was put in likely signals and listened to find out if they succeeded. The results of scanning were circulated to other phreaks. Discovering each other took time at first, but evenutally the phreaks became organized. The "TAP" of Britain was called "Undercurrents" which enabledBritish phreaks to share the info on new numbers, equipment etc. To understand what the British british phreaks did, think of the phonenetowrk in three layers of lines: Local, trunk, and international. In the UK, Subcriber Trunk Dialing (STD), is the mechanism which takes a call from the local lines and (legitimately) elevates it to a trunk or internationallevel. The UK phreaks figured that a call at trunk level can be routed through any number of exchanges, provided that the right routing codes were found and used correctly. They also had to discover how to get from local to trunk level either without being charged (which they did with a bleeper box) or without using (STD). Chaining has already been mentioned but it requires long strings of digits and speech gets more and more faint as the chain grows, just likeit does when you stack trunks back and forth accross the U.S. The way the security reps snagged the phreaks was to put a

simple 'printermeter' or as we call it: a pen register on the suspects line, which shows every digit dialedfrom the subscribers line. The British prefer to get onto the trunks rather than chaining. One way was to discover where local calls use the trunks between neighboring exchanges, start a call and stay on the trunk instead of returning to the local level on reaching the distant switch. This again required exhaustive dialing and made more work for Titan; it also revealed 'fiddles', which were inserted by Post Office Engineers. What fiddling means is that the engineers rewired the exchanges for thier own benefit. The equipment is modified to give access to a trunk with out being charged, an operation which is pretty easy in Step by Step(SXS) electromechanical exchanges, which were installed in Britain even in the
1970s (NOTE: I know of a back door into the Canadian system on a 4A CO., so if you are on SXS or a 4A, try scanning 3 digit exchanges, ie: dial 999,998,997 etc. and listen for the beep-kerchink, if there are no 3 digit codes which allow direct access to a tandem in your local exchange and bypasses the AMA so you won't be billed, not have to blast 2600 every time you wish to box a call. A famous British 'fiddler' revealed in the early 1970s worked by dialing 173.The caller then added the trunk code of 1 and the subscribers local number. At that time, most engineering test services began with 17X, so the engineers could hide thier fiddles in the nest of service wires. When security reps started searching, the fiddles were concealed by tones signalling: 'number unobtainalbe' or 'equipment engaged' which switched off after a delay. The necessary relays are small and easily hidden. $There was another side to phreaking In the UK in the sixties. Before STD was widespread, many 'ordinary' people were driven to occasional phreaking from sheer frustration at the inefficient operator controlled trunk system.This came to a head during a strike about 1961 when operators could not be reached. Nothing complicated was needed. Many operators had been in the habit of repeating the codes as they dialled the requested numbers so people soon learnt the numbers they called frequently. The only 'trick' was to know which exchanges could be dialled through to pass on the trunk number. Callers also needed a pretty quiet place to do it, since timing relative to clicks was important The most famous trial of British phreaks was called the Old Baily trial. Whichstarted on 3 Oct. 1973. What they phreaks did was to dial a spare number at a local call rate but involving a trunk to another exchange Then they send a 'clear forward' to thier local exchange, indicating to it that the call is finished;but the distant exchange doesn't realize because the caller's phone isstill Off the hook. They now have an open line into the distant trunk exchange and sends to it a 'seize' signal: '1' which puts him onto its outgoing lines.Now, if they know the codes, the world is open to them. All other exchanges trust his local exchange to handle the billing; they just interpret the tones they hear. Mean while, the local exchange collects only for a local call. Theinvestigators discovered the phreaks holding a conference somewhere in England surrounded by various phone equipment and bleeper boxes, also printouts listing'secret' Post Office codes. (They probably got them from trashing?) The judge said: "some take to heroin, some take to telephones" for them phone phreakingwas not a crime but a hobby to be shared with phellow enthusists and discussed with the Post Office openly over dinner and by mail. Their approach and attitude to the worlds larges computer, the global telephone system, was that of scientist s conducting experiments or programmers and engineers testing programs and systems. The judge apeared to agree, and even asked

them for phreaking codes to use from his local exchange!!!