The Catman's Lair

Hacker Resource Files

http://www.pryde-lands.com/catman/

WARNING - Contents of this file are for educational purposes only. It is strongly suggested that you do not use this knowledge for illegal purposes!

Century Communications

- T H E -

- H A C K E R ' S -

- H A N D B O O K -

First published in Great Britain in 1985 by Century Communications Ltd
Portland House, 12-13 Greek Street, London W1V 5LE.

Reprinted 1985 (four times)

ISBN 0 7126 0650 5

Printed and bound in Great Britain by Billing & Sons Limited, Worcester.

CONTENTS

INTRODUCTION

The word 'hacker' is used in two different but associated ways: for some, a hacker is merely a computer enthusiast of any kind, who loves working with the beasties for their own sake, as opposed to operating them in order to enrich a company or research project --or to play games.

This book uses the word in a more restricted sense: hacking is a recreational and educational sport. It consists of attempting to make unauthorised entry into computers and to explore what is there. The sport's aims and purposes have been widely misunderstood; most hackers are not interested in perpetrating massive frauds, modifying their personal banking, taxation and employee records, or inducing one world super-power into inadvertently commencing Armageddon in the mistaken belief that another super-power is about to attack it. Every hacker I have ever come across has been quite clear about where the fun lies: it is in developing an understanding of a system and finally producing the skills and tools to defeat it. In the vast majority of cases, the process of 'getting in' is much more satisfying than what is discovered in the protected computer files.

In this respect, the hacker is the direct descendant of the phone phreaks of fifteen years ago. Phone phreaking became interesting as intra-nation and international subscriber trunk dialling was introduced, but when the London-based phreak finally chained his way through to Hawaii, he usually had no one there to speak to except the local weather service or American Express office, to confirm that the desired target had indeed been hit. One of the earliest of the present generation of hackers, Susan Headley, only 17 when she began her exploits in California in 1977, chose as her target the local phone company and, with the information extracted from her hacks, ran all over the telephone network. She 'retired' four years later, when friends started developing schemes to shut down part of the phone system.

There is also a strong affinity with program copy-protection crunchers. Most commercial software for micros is sold in a form to prevent obvious casual copying, say by loading a cassette, cartridge or disk into memory and then executing a 'save' on to a

blank cassette or disk. Copy-protection devices vary greatly in their methodology and sophistication and there are those who, without any commercial motive, enjoy nothing so much as defeating them. Every computer buff has met at least one cruncher with a vast store of commercial programs, all of which have somehow had the protection removed--and perhaps the main title subtly altered to show the cruncher's technical skills--but which are then never actually used at all.

Perhaps I should tell you what you can reasonably expect from this handbook. Hacking is an activity like few others: it is semi-legal, seldom encouraged, and in its full extent so vast that no individual or group, short of an organisation like GCHQ or NSA, could hope to grasp a fraction of the possibilities. So this is not one of those books with titles like Games Programming with the 6502 where, if the book is any good and if you are any good, you will emerge with some mastery of the subject-matter. The aim of this book is merely to give you some grasp of methodology, help you develop the appropriate attitudes and skills, provide essential background and some referencing material--and point you in the right directions for more knowledge. Up to a point, each chapter may be read by itself; I have compiled extensive appendices, containing material which will be of use long after the main body of the text has been absorbed.

It is one of the characteristics of hacking anecdotes, like those relating to espionage exploits, that almost no one closely involved has much stake in the truth; victims want to describe damage as minimal, and perpetrators like to paint themselves as heroes while carefully disguising sources and methods. In addition, journalists who cover such stories are not always sufficiently competent to write accurately, or even to know when they are being hoodwink- ed. (A note for journalists: any hacker who offers to break into a system on demand is conning you--the most you can expect is a repeat performance for your benefit of what a hacker has previously succeeded in doing. Getting to the 'front page' of a service or network need not imply that everything within that service can be accessed. Being able to retrieve confidential information, perhaps credit ratings, does not mean that the hacker would also be able to alter that data. Remember the first rule of good reporting: be sceptical.) So far as possible, I have tried to verify each story that appears in these pages, but hackers work in isolated groups and my sources on some of the important hacks of recent years are more remote than I would have liked. In these

cases, my accounts are of events and methods which, in all the circumstances, I believe are true. I welcome notes of correction.

Experienced hackers may identify one or two curious gaps in the range of coverage, or less than full explanations; you can chose any combination of the following explanations without causing me any worry: first, I may be ignorant and incompetent; second, much of the fun of hacking is making your own discoveries and I wouldn't want to spoil that; third, maybe there are a few areas which are really best left alone.

Nearly all of the material is applicable to readers in all countries; however, the author is British and so are most of his experiences.

The pleasures of hacking are possible at almost any level of computer competence beyond rank beginner and with quite minimal equipment. It is quite difficult to describe the joy of using the world's cheapest micro, some clever firmware, a home-brew acoustic coupler and find that, courtesy of a friendly remote PDP11/70, you

can be playing with Unix, the fashionable multitasking operating system.

The assumptions I have made about you as a reader are that you own a modest personal computer, a modem and some communications software which you know, roughly, how to use. (If you are not confident yet, practise logging on to a few hobbyist bulletin boards.) For more advanced hacking, better equipment helps; but, just as very tasty photographs can be taken with snap-shot cameras, the computer equivalent of a Hasselblad with a trolley- load of accessories is not essential.

Since you may at this point be suspicious that I have vast technical resources at my disposal, let me describe the kit that has been used for most of my network adventures. At the centre is a battered old Apple II+, its lid off most of the time to draw away the heat from the many boards cramming the expansion slots. I use an industry standard dot matrix printer, famous equally for the variety of type founts possible, and for the paper-handling path, which regularly skews off. I have two large boxes crammed full of software, as I collect comms software in particular like a deranged philatelist, but I use one package almost exclusively. As for modems--well, at this point the set-up does become unconventional; by the phone point are jack sockets for BT 95A, BT 96A, BT 600 and a North American modular jack. I have two acoustic couplers, devices for plunging telephone handsets into so that the computer can talk down the line, at operating speeds of 300/300 and 75/1200. I also have three heavy, mushroom coloured 'shoe-boxes', representing modem technology of 4 or 5 years ago and operating at various speeds and combinations of duplex/half- duplex. Whereas the acoustic coupler connects my computer to the line by audio, the modem links up at the electrical level and is more accurate and free from error. I have access to other equipment in my work and through friends, but this is what I use most of the time.

Behind me is my other important bit of kit: a filing cabinet. Hacking is not an activity confined to sitting at keyboards and watching screens. All good hackers retain formidable collections of articles, promotional material and documentation; read on, and you will see why.

Finally, to those who would argue that a hacker's handbook must be giving guidance to potential criminals, I have two things to say: First, few people object to the sports of clay-pigeon shooting or archery, although rifles, pistols and crossbows have no 'real' purpose other than to kill things--and hackers have their own code of responsibility, too. Second, real hacking is not as it is shown in the movies and on tv, a situation which the publication of this book may do something to correct. The sport of hacking itself may involve breach of aspects of the law, notably theft of electricity, theft of computer time and unlicensed usage of copyright material; every hacker must decide individually each instance as it arises.

Various people helped me on various aspects of this book; they must all remain unnamed--they know who they are and that they have my

thanks.

** Page X

CHAPTER 1

First Principles

The first hack I ever did was executed at an exhibition stand run by BT's then rather new Prestel service. Earlier, in an adjacent conference hall, an enthusiastic speaker had demonstrated view-data's potential world-wide spread by logging on to Viditel, the infant Dutch service. He had had, as so often happens in the these circumstances, difficulty in logging on first time. He was using one of those sets that displays auto-dialled telephone numbers; that was how I found the number to call. By the time he had finished his third unsuccessful log-on attempt I (and presumably several others) had all the pass numbers. While the BT staff were busy with other visitors to their stand, I picked out for myself a relatively neglected viewdata set. I knew that it was possible to by-pass the auto-dialler with its pre-programmed phone numbers in this particular model, simply by picking up the the phone adjacent to it, dialling my preferred number, waiting for the whistle, and then hitting the keyboard button labelled 'viewdata'. I dialled Holland, performed my little by-pass trick and watched Viditel write itself on the screen. The pass numbers were accepted first time and, courtesy of...no, I'll spare them embarrassment...I had only lack of fluency in Dutch to restrain my explorations. Fortunately, the first BT executive to spot what I had done was amused as well.

Most hackers seem to have started in a similar way. Essentially you rely on the foolishness and inadequate sense of security of computer salesmen, operators, programmers and designers.

In the introduction to this book I described hacking as a sport; and like most sports, it is both relatively pointless and filled with rules, written or otherwise, which have to be obeyed if there is to be any meaningfulness to it. Just as rugby football is not only about forcing a ball down one end of a field, so hacking is not just about using any means to secure access to a computer.

On this basis, opening private correspondence to secure a password on a public access service like Prestel and then running around the system building up someone's bill, is not what hackers call hacking. The critical element must be the use of skill in some shape or form.

** Page 1

Hacking is not a new pursuit. It started in the early 1960s when the first "serious" time-share computers began to appear at university sites. Very early on, 'unofficial' areas of the memory started to appear, first as mere notice boards and scratch pads for private programming experiments, then, as locations for games. (Where, and how do you think the early Space Invaders, Lunar Landers

and Adventure Games were created?) Perhaps tech-hacking-- the mischievous manipulation of technology--goes back even further. One of the old favourites of US campus life was to rewire the control panels of elevators (lifts) in high-rise buildings, so that a request for the third floor resulted in the occupants being whizzed to the twenty-third.

Towards the end of the 60s, when the first experimental networks arrived on the scene (particularly when the legendary ARPAnet--Advanced Research Projects Agency network-- opened up), the computer hackers skipped out of their own local computers, along the packet-switched high grade communications lines, and into the other machines on the net. But all these hackers were privileged individuals. They were at a university or research resource, and they were able to borrow terminals to work with.

What has changed now, of course, is the wide availability of home computers and the modems to go with them, the growth of public-access networking of computers, and the enormous quantity and variety of computers that can be accessed.

Hackers vary considerably in their native computer skills; a basic knowledge of how data is held on computers and can be transferred from one to another is essential. Determination, alertness, opportunism, the ability to analyse and synthesise, the collection of relevant helpful data and luck--the pre-requisites of any intelligence officer--are all equally important. If you can write quick effective programs in either a high level language or machine code, well, it helps. A knowledge of on-line query procedures is helpful, and the ability to work in one or more popular mainframe and mini operating systems could put you in the big league.

The materials and information you need to hack are all around you--only they are seldom marked as such. Remember that a large proportion of what is passed off as 'secret intelligence' is openly available, if only you know where to look and how to appreciate what you find. At one time or another, hacking will test everything you know about computers and communications. You will discover your abilities increase in fits and starts, and you must

be prepared for long periods when nothing new appears to happen.

Popular films and tv series have built up a mythology of what hackers can do and with what degree of ease. My personal delight in such Dream Factory output is in compiling a list of all the mistakes in each episode. Anyone who has ever tried to move a graphics game from one micro to an almost-similar competitor will already know that the chances of getting a home micro to display the North Atlantic Strategic Situation as it would be viewed from the President's Command Post would be slim even if appropriate telephone numbers and passwords were available. Less immediately obvious is the fact that most home micros talk to the outside world through limited but convenient asynchronous protocols, effectively denying direct access to the mainframe products of the world's undisputed leading computer manufacturer, which favours synchronous protocols. And home micro

displays are memory-mapped, not vector-traced... Nevertheless, it is astonishingly easy to get remarkable results. And thanks to the protocol transformation facilities of PADs in PSS networks (of which much more later), you can get into large IBM devices....

The cheapest hacking kit I have ever used consisted of a ZX81, 16K RAMpack, a clever firmware accessory and an acoustic coupler. Total cost, just over ú100. The ZX81's touch-membrane keyboard was one liability; another was the uncertainty of the various connectors. Much of the cleverness of the firmware was devoted to overcoming the native drawbacks of the ZX81's inner configuration--the fact that it didn't readily send and receive characters in the industry-standard ASCII code, and that the output port was designed more for instant access to the Z80's main logic rather than to use industry-standard serial port protocols and to rectify the limited screen display.

Yet this kit was capable of adjusting to most bulletin boards; could get into most dial-up 300/300 asynchronous ports, re-configuring for word-length and parity if needed; could have accessed a PSS PAD and hence got into a huge range of computers not normally available to micro-owners; and, with another modem, could have got into viewdata services. You could print out pages on the ZX 'tin-foil' printer. The disadvantages of this kit were all in convenience, not in facilities. Chapter 3 describes the sort of kit most hackers use.

It is even possible to hack with no equipment at all. All major banks now have a network of 'hole in the wall' cash machines-- ATMs or Automatic Telling Machines, as they are officially

known. Major building societies have their own network. These machines have had faults in software design, and the hackers who played around with them used no more equipment than their fingers and brains. More about this later.

Though I have no intention of writing at length about hacking etiquette, it is worth one paragraph: lovers of fresh-air walks obey the Country Code; they close gates behind them, and avoid damage to crops and livestock. Something very similar ought to guide your rambles into other people's computers: don't manipulate files unless you are sure a back-up exists; don't crash operating systems; don't lock legitimate users out from access; watch who you give information to; if you really discover something confidential, keep it to yourself. Hackers should not be interested in fraud. Finally, just as any rambler who ventured past barbed wire and notices warning about the Official Secrets Acts would deserve whatever happened thereafter, there are a few hacking projects which should never be attempted.

On the converse side, I and many hackers I know are convinced of one thing: we receive more than a little help from the system managers of the computers we attack. In the case of computers owned by universities and polys, there is little doubt that a number of them are viewed like academic libraries--strictly speaking they are for

the student population, but if an outsider seriously thirsty for knowledge shows up, they aren't turned away. As for other computers, a number of us are almost sure we have been used as a cheap means to test a system's defences...someone releases a phone number and low-level password to hackers (there are plenty of ways) and watches what happens over the next few weeks while the computer files themselves are empty of sensitive data. Then, when the results have been noted, the phone numbers and passwords are changed, the security improved etc etc....much easier on dp budgets than employing programmers at £150/man/ day or more. Certainly the Pentagon has been known to form 'Tiger Units' of US Army computer specialists to pin-point weaknesses in systems security.

Two spectacular hacks of recent years have captured the public imagination: the first, the Great Prince Philip Prestel Hack, is described in detail in chapter 8, which deals with viewdata. The second was spectacular because it was carried out on live national television. It occurred on October 2nd 1983 during a follow-up to the BBC's successful Computer Literacy series. It's worth reporting here, because it neatly illustrates the essence of hacking as a sport... skill with systems, careful research, maximum impact

with minimum real harm, and humour.

The tv presenter, John Coll, was trying to show off the Telecom Gold electronic mail service. Coll had hitherto never liked long passwords and, in the context of the tight timing and pressures of live tv, a two letter password seemed a good idea at the time. On Telecom Gold, it is only the password that is truly confidential; system and account numbers, as well as phone numbers to log on to the system, are easily obtainable. The BBC's account number, extensively publicised, was OWL001, the owl being the 'logo' for the tv series as well as the BBC computer.

The hacker, who appeared on a subsequent programme as a 'former hacker' and who talked about his activities in general, but did not openly acknowledge his responsibility for the BBC act, managed to seize control of Coll's mailbox and superimpose a message of his own:

Computer Security Error. Illegal access. I hope your television PROGRAMME runs as smoothly as my PROGRAM worked out your passwords! Nothing is secure!

Hackers' Song

"Put another password in,
Bomb it out and try again
Try to get past logging in,
We're hacking, hacking, hacking

Try his first wife's maiden name,
This is more than just a game,
It's real fun, but just the same,

It's hacking, hacking, hacking"

The Nutcracker (Hackers UK)

HI THERE, OWLETS, FROM OZ AND YUG
(OLIVER AND GUY)

After the hack a number of stories about how it had been carried out, and by whom, circulated; it was suggested that the hackers had crashed through to the operating system of the Prime computers upon which the Dialcom electronic mail software

** Page 5

resided--it was also suggested that the BBC had arranged the whole thing as a stunt, or alternatively, that some BBC employees had fixed it up without telling their colleagues. Getting to the truth of a legend in such cases is almost always impossible. No one involved has a stake in the truth. British Telecom, with a strong commitment to get Gold accepted in the business community, was anxious to suggest that only the dirtiest of dirty tricks could remove the inherent confidentiality of their electronic mail service. Naturally, the British Broadcasting Corporation rejected any possibility that it would connive in an irresponsible cheap stunt. But the hacker had no great stake in the truth either--he had sources and contacts to protect, and his image in the hacker community to bolster. Never expect any hacking anecdote to be completely truthful.

** Page 6

CHAPTER 2

Computer-to-Computer
Communications

Services intended for access by microcomputers are nowadays usually presented in a very user-friendly fashion: pop in your software disc or firmware, check the connections, dial the telephone number, listen for the tone...and there you are. Hackers, interested in venturing where they are not invited, enjoy no such luxury. They may want to access older services which preceded the modern 'human interface'; they are very likely to travel along paths intended, not for ordinary customers, but for engineers or salesmen; they could be utilising facilities that were part of a computer's commissioning process and have been hardly used since.

So the hacker needs a greater knowledge of datacomms technology than does a more passive computer user, and some feeling for the history of the technology is pretty essential, because of its growth pattern and because of the fact that many interesting installations still use yesterday's solutions.

Getting one computer to talk to another some distance away means accepting a number of limiting factors:

* Although computers can send out several bits of information at once, the ribbon cable necessary to do this is not economical at any great length, particularly if the information is to be sent out over a network--each wire in the ribbon would need switching separately, thus making ex- changes prohibitively expensive. So bits must be transmitted one at a time, or serially.

** Page 7

* Since you will be using, in the first instance, wires and networks already installed--in the form of the telephone and telex networks--you must accept that the limited bandwidth of these facilities will restrict the rate at which data can be sent. The data will pass through long lengths of wire, frequently being re-amplified, and undergoing de- gradation as it passes through dirty switches and relays in a multiplicity of exchanges.

* Data must be easily capable of accurate recovery at the far end.

* Sending and receiving computers must be synchronised in their working.

* The mode in which data is transmitted must be one understood by all computers; accepting a standard protocol may mean adopting the speed and efficiency of the slowest.

* The present 'universal' standard for data transmission used by microcomputers and many other services uses agreed tones to signify binary 0 and binary 1, the ASCII character set (also known as International Alphabet No 5), and an asynchronous protocol, whereby the transmitting and receiving computers are locked in step every time a character is sent, not just at the beginning of a transmission stream. Like nearly all standards, it is highly arbitrary in its decisions and derives its importance simply from the fact of being generally accepted. Like many standards, too, there are a number of subtle and important variations.

To see how the standard works, how it came about and the reasons for the variations, we need to look back a little into history.

The Growth of Telegraphy

The essential techniques of sending data along wires has a history of 150 years, and some of the common terminology of modern data transmission goes right back to the first experiments.

The earliest form of telegraphy, itself the earliest form of electrical message sending, used the remote actuation of electrical relays to leave marks on a strip of paper. The letters of the alphabet were defined by the patterns of 'mark' and 'space'.

** Page 8

The terms have come through to the present, to signify binary conditions of '1' and '0' respectively. The first reliable machine

for sending letters and figures by this method dates from 1840; the direct successor of that machine, using remarkably unchanged electromechanical technology and a 5-bit alphabetic code, is still widely used today, as the telex/teleprinter/teletype. The mark and space have been replaced by holes punched in paper-tape: larger holes for mark, smaller ones for space. Synchronisation between sending and receiving stations is carried out by beginning each letter with a 'start' bit (a space) and concluding it with a 'stop' bit (mark). The 'idle' state of a circuit is thus 'mark'. In effect, therefore, each letter requires the transmission of 7 bits:

. * * . . . * (letter A: . = space; * = mark)

of which the first . is the start bit, the last * is the stop bit and * * . .. is the code for A.

This is the principle means for sending text messages around the world, and the way in which news reports are distributed globally. And, until third-world countries are rich enough to afford more advanced devices, the technology will survive.

Early computer communications

When, 110 years after the first such machines came on line, the need arose to address computers remotely, telegraphy was the obvious way to do so. No one expected computers in the early 1950s to give instant results; jobs were assembled in batches, often fed in by means of paper-tape (another borrowing from telex, still in use) and then run. The instant calculation and collation of data was then considered quite miraculous. So the first use of data communications was almost exclusively to ensure that the machine was fed with up-to-date information, not for the machine to send the results out to those who might want it; they could wait for the 'print-out' in due course, borne to them with considerable solemnity by the computer experts. Typical communications speeds were 50 or 75 baud. (The baud is the measure of speed of data transmission: specifically, it refers to the number of signal level changes per second and is thus not the same as bits-per-second.)

These early computers were, of course, in today's jargon, single-user/single-task; programs were fed by direct machine coding. Gradually, over the next 15 years, computers spawned multi-user capabilities by means of time-sharing techniques, and their human interface became more 'user-friendly'.

With these facilities grew the demand for remote access to computers, and modern data communications began.

Even at the very end of the 1960s when I had my own very first encounter with a computer, the links with telegraphy were still obvious. As a result of happenstance, I was in a Government-run research facility to the south-west of London, and the program I was to use was located on a computer just to the north of Central London; I was sat down in front of a battered teletype--capitals and figures

only, and requiring not inconsiderable physical force from my smallish fingers to actuate the keys of my choice. As it was a teletype outputting on to a paper roll, mistakes could not as readily be erased as on a VDU, and since the sole form of error reporting consisted of a solitary ?, the episode was more frustrating than thrilling. VDUs and good keyboards were then far too expensive for 'ordinary' use.

The telephone network

But by that time all sorts of changes in datacomms were taking place. The telex and telegraphy network, originally so important, had long been overtaken by voice-grade telephone circuits (Bell's invention dates from 1876). For computer communication, mark and space could be indicated by different audio tones, rather than by different voltage conditions. Data traffic on a telex line can operate in only one direction at a time, but, by selecting different pairs of tones, both 'transmitter' and 'receiver' could speak simultaneously--so that in fact, one has to talk about 'originate' and 'answer' instead.

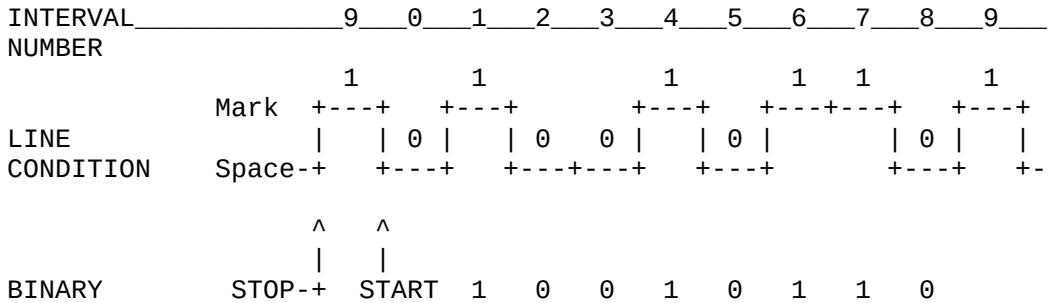
Improved electrical circuit design meant that higher speeds than 50 or 75 baud became possible; there was a move to 110 baud, then 300 and, so far as ordinary telephone circuits are concerned, 1200 baud is now regarded as the top limit.

The 'start' and 'stop' method of synchronising the near and far end of a communications circuit at the beginning of each individual letter has been retained, but the common use of the 5-bit Baudot code has been replaced by a 7-bit extended code which allows for many more characters, 128 in fact.

Lastly, to reduce errors in transmission due to noise in the telephone line and circuitry, each letter can be checked by the use of a further bit (the parity bit), which adds up all the bits in the main character and then, depending on whether the result is odd or even, adds a binary 0 or binary 1.

The full modern transmission of a letter in this system, in this case, K, therefore, looks like this:

START-STOP TRANSMISSION OF A DATA CHARACTER



The first 0 is the start bit; then follows 7 bits of the actual letter code (1001011); then the parity bit; then the final 1 is the stop code.

This system, asynchronous start-stop ASCII (the common name for the alphabetic code), is the basis for nearly all micro-based communications. The key variations relate to:

bit-length; you can have 7 or 8 databits (*)

parity; (it can be even or odd, or entirely absent),

Tones - The tones used to signify binary 0 and binary 1, and which computer is in 'originate' and which in 'answer', can vary according to the speed of the transmission and also to whether the service is used in North America or the rest of the world. (Briefly, most of the world uses tones and standards laid down by the Geneva-based organisation, CCITT, a specialised agency of the International Telecommunications Union; whereas in the United States and most parts of Canada, tones determined by the telephone utility, colloquially known as Ma Bell, are adopted.) The following table gives the standards and tones in common use.

(*) There are no 'obvious explanations' for the variations commonly found: most electronic mail services and viewdata transmit 7 data bits, even parity and I stop Bit; Telecom Gold and most hobbyist bulletin boards transmit 8 data bits, odd parity and 1 stop bit. Terminal emulator software--see chapter 3--allows users to adjust for these differing requirements.

Service Designator	Speed	Duplex	Transmit 0	Transmit 1	Receive 0	Receive 1	Answer
V21 orig	300(*)	full	1180	980	1850	1650	-
V21 ans	300(*)	full	1850	1650	1180	980	2100
V23 (1)	600	half	1700	1300	1700	1300	2100
V23 (2)	1200	f/h(**)	2100	1300	2100	1300	2100
V23 back	75	f/h(**)	450	390	450	390	-
Bell 103 orig	300(*)	full	1070	1270	2025	2225	-
Bell 103 ans	300(*)	full	2025	2225	1070	1270	2225
Bell 202	1200	half	2200	1200	2200	1200	2025

(*)any speed up to 300 baud, can also include 75 and 110 baud services

(**)service can either be half-duplex at 1200 baud or asymmetrical full duplex, with 75 baud originate and 1200 baud receive (commonly used as viewdata user) or 1200 transmit and 75 receive (viewdata host)

Higher Speeds

1200 baud is usually regarded as the fastest speed possible on an ordinary voice-grade telephone line. Beyond this, noise on the line due to the switching circuits at the various telephone exchanges, poor cabling, etc. make accurate transmission difficult. Indeed, at higher speeds it becomes increasingly important to use transmission protocols that include error correction.

Error correction techniques usually consist of dividing the transmission stream into a series of blocks which can be checked, one at a time, by the receiving computer. The 'parity' system mentioned above is one example, but obviously a crude one. The difficulty is that the more secure an error-correction protocol becomes, the greater becomes the overhead in terms of numbers of bits transmitted to send just one character from one computer to another. Thus, in the typical 300 bit situation, the actual letter is defined by 7 bits, 'start' and 'stop' account for another two, and the check takes a further one--ten in all. After a while, what you gain in the speed with which each actual bit is transmitted, you lose, because so many bits have to be sent to ensure that a single character is accurately received!

Although some people risk using 2400 baud on ordinary telephone lines--the jargon is the PTSN (Public Telephone Switched Network)--this means using expensive modems. Where higher speeds are essential, leased circuits, not available via dial-up. become essential. The leased circuit is paid for on a fixed charge, not a charge based on time-connected. Such circuits can be conditioned', for example by using special amplifiers, to support the higher data rate.

For really high speed transmissions, however, pairs of copper cable are inadequate. Medium speed is obtainable by the use of coaxial cable (a little like that used for tv antenna hook-ups) which have a very broad bandwidth. Imposing several different channels on one cable-length is called multiplexing and, depending on the application, the various channels can either carry several different computer conversations simultaneously or can send several bits of one computer conversation in parallel, just as though there were a ribbon cable between the two participating computers. Either way, what happens is that each binary 0 or binary 1 is given, not an audio tone, but a radio frequency tone.

Synchronous Protocols

In the asynchronous protocols so far described, transmitting and receiving computers are kept in step with each other every time a character is sent, via the 'start' and 'stop' bits. In synchronous comms, the locking together is done merely at the start of each block of transmission by the sending of a special code (often SYN). The SYN code starts a clock (a timed train of pulses) in the receiver and it is this that ensures that binary 0s and 1s originating at the transmitter are correctly interpreted by the receiver; clearly, the displacement of even one binary digit can cause havoc.

A variety of synchronous protocols exist, such as the length of block sent each time, the form of checking that takes place, the form of acknowledgement, and so on. A synchronous protocol is not only a function of the modem, which has to have a suitable clock, but also of the software and firmware in the computers. Because asynchronous protocols transmit so many 'extra' bits in order to avoid error, savings in transmission time under synchronous systems often exceed 20-30%. The disadvantage of synchronous protocols lie in increased hardware costs.

One other complication exists: most asynchronous protocols use the ASCII code to define characters. IBM ('Big Blue'), the biggest enthusiast of synchronous comms, has its own binary code to define characters. In Appendix IV, you will find an explanation and a comparison with ASCII.

** Page 13

The hacker, wishing to come to terms with synchronous comms, has two choices: the more expensive is to purchase a protocol convertor board. These are principally available for the IBM PC, which has been increasingly marketed for the 'executive workstation' audience, where the ability to interface to a company's existing (IBM) mainframe is a key feature. The alternative is to see whether the target mainframe has a port on to a packet- switched service; in that event, the hacker can use ordinary asynchronous equipment and protocols--the local PAD (Packet Assembler/Disassembler) will carry out the necessary transformations.

Networks

Which brings us neatly to the world of high-speed digital networks using packet-switching. All the computer communications so far described have taken place either on the phone (voice-grade) network or on the telex network.

In Chapter 7 we will look at packet-switching and the opportunities offered by international data networks. We must now specify hackers' equipment in more detail.

** Page 14

CHAPTER 3

Hackers' Equipment

You can hack with almost any microcomputer capable of talking to the outside world via a serial port and a modem. In fact, you don't even need a micro; my first hack was with a perfectly ordinary viewdata terminal.

What follows in this chapter, therefore, is a description of the elements of a system I like to think of as optimum for

straight-forward asynchronous ASCII and Baudot communications. What is at issue is convenience as much as anything. With kit like this, you will be able to get through most dial-up ports and into packet-switching through a PAD -- a packet assembler/ disassembler port. (It will not get you into IBM networks, because these use different and incompatible protocols; we will return to the matter of the IBM world in chapter 10.) In other words, given a bit of money, a bit of knowledge, a bit of help from friends and a bit of luck, what is described here is the sort of equipment most hackers have at their command.

You will find few products on the market labelled 'for hackers'; you must select those items that appear to have 'legitimate' but interesting functions and see if they can be bent to the hacker's purposes. The various sections within this chapter highlight the sort of facilities you need; before lashing out on some new software or hardware, try to get hold of as much publicity and documentation material as possible to see how adaptable the products are. In a few cases, it is worth looking at the second-hand market, particularly for modems, cables and test equipment.

Although it is by no means essential, an ability to solder a few connections and scrabble among the circuit diagrams of 'official' products often yield unexpectedly rewarding results.

The computer

Almost any popular microcomputer will do; hacking does not call upon enormous reserves of computer power. Nearly everything you hack will come to you in alphanumeric form, not graphics. The computer you already have will almost certainly have the essential qualities. However the very cheapest micros, like the ZX81, whilst usable, require much more work on the part of the operator/hacker, and give him far less in the way of instant facilities.

(In fact, as the ZX81 doesn't use ASCII internally, but a Sinclair-developed variant; you will need a software or firmware fix for that, before you even think of hooking it up to a modem.)

Most professional data services assume the user is viewing on an 80-column screen; ideally the hacker's computer should be capable of doing that as well, otherwise the display will be full of awkward line breaks. Terminal emulator software (see below) can some- times provide a 'fix'.

One or two disc drives are pretty helpful, because you will want to be able to save the results of your network adventures as quickly and efficiently as possible. Most terminal emulators use the computer's free memory (i.e. all that is not required to support the operating system and the emulator software itself) as store for the received data, but once the buffer is full, you will begin to lose the earliest items. You can, of course, try to save to cassette, but normally that is a slow and tedious process.

An alternative storage method is to save to a printer, printing the received data stream not only to the computer screen, but also on a dot matrix printer. However, most of the more popular (and cheaper) printers do not work sufficiently fast. You may find you lose characters at the beginning of each line. Moreover, if you print everything in real-time, you'll include all your mistakes, false starts etc., and in the process use masses of paper. So, if you can save to disc regularly, you can review each hack afterwards at your leisure and, using a screen editor or word processor, save or print out only those items of real interest.

Serial ports

The computer must have a serial port, either called that or marked RS232C (or its slight variant RS423), or V24, which is the official designator of RS232C used outside the USA, though not often seen on micros.

The very cheapest micros, like the ZX81, Spectrum, VIC20, do not have RS232C ports, though add-on boards are available. Some of the older personal computers, like the Apple or the original Pet, were also originally sold without serial ports, though standard boards are available for all of these.

You are probably aware that the RS232C standard has a large number of variants, and that not all computers (or add-on boards) that claim to have a RS232C port can actually talk into a modem.

Historically, RS232C/V24 is supposed to cover all aspects of serial communication, including printers and dumb terminals as well as computers. The RS232C standard specifies electrical and physical requirements.

Everything is pumped through a 25-pin D-shaped connector, each pin of which has some function in some implementation. But in most cases, nearly all the pins are not used. In practice, only three connections are essential for computer to modem communication:

Pin 7 signal ground

Pin 2 characters leaving the computer

Pin 3 characters arriving at the computer

The remaining connections are for such purposes as feeding power to an external device, switching the external advice on or off, exchanging status and timing signals, monitoring the state of the line, and so forth. Some computers and their associated firmware require one or other of these status signals to go 'high' or 'low' in particular circumstances, or the program hangs. Check your documentation if you have trouble.

Some RS232C implementations on microcomputers or add-on boards are there simply to support printers with serial interfaces, but they can

often be modified to talk into modems. The critical two lines are those serving Pins 2 and 3.

A computer serving a modem needs a cable in which Pin 2 on the computer is linked to Pin 2 on the modem.

A computer serving a printer, etc, needs a cable in which Pin 3 on the: computer is linked to Pin 2 on the printer and Pin 3 on the printer is linked to Pin 2 on the computer.

If two computers are linked together directly, without a modem, then Pin 2 on computer A must be linked to Pin 3 on computer B and Pin 3 on computer B linked to Pin 2 on computer A: this arrangement is sometimes called a 'null modem' or a 'null modem cable'.

There are historic explanations for these arrangements, depending on who you think is sending and who is receiving--forget about them, they are confusing. The above three cases are all you need to know about in practice.

One difficulty that frequently arises with newer or portable computers is that some manufacturers have abandoned the traditional 25-way D-connector, largely on the grounds of bulk, cost and redundancy. Some European computer and peripheral companies favour connectors based on the DIN series (invented in Germany), while others use D-connectors with fewer pin-outs.

There is no standardisation. Even if you see two physically similar connectors on two devices, regard them with suspicion. In each case, you must determine the equivalents of:

Characters leaving computer (Pin 2)
Characters arriving at computer (Pin 3)
Signal ground (Pin 7)

You can usually set the speed of the port from the computer's operating system and/or from Basic. There is no standard way of doing this; you must check your handbook and manuals. Most RS232C ports can handle the following speeds:

75, 110, 300, 600, 1200, 2400, 4800, 9600

and sometimes 50 and 19200 baud as well. These speeds are selectable in hardware by appropriate wiring of a chip called a baud-rate generator. Many modern computers let you select speed in hardware by means of a DIL switch. The higher speeds are used either for driving printers or for direct computer-to-computer or computer-to-peripheral connections. The normal maximum speed for transmitting along phone lines is 1200 baud.

Depending on how your computer has been set up, you may be able to control the speed from the keyboard--a bit of firmware in the computer will accept micro-instructions to flip transistor switches controlling the wiring of the baud-rate generator. Alternatively,

the speeds may be set in pure software, the micro deciding at what speed to feed information into the serial port.

In most popular micro implementations the RS232C cannot support split-speed working (different speeds for receive and transmit). If you set the port up for 1200 baud, it has to be 1200 receive and transmit. This is a nuisance in Europe, where 75/1200 is in common use both for viewdata systems and for some on-line services. The usual way round is to have special terminal emulator software, which requires the RS232C hardware to operate at 1200 /1200 and then slows down (usually the micro's transmit path) to 75 baud in software by means of a timing loop. An alternative method relies on a special modem, which accepts data from the computer at 1200/1200 and then performs the slowing-down to 75 baud in its own internal firmware.

Terminal emulators

We all need a quest in life. Sometimes I think mine is to search for the perfect software package to make micros talk to the outside world.

As in all such quests, the goal is occasionally approached but never reached, if only because the process of the quest causes one to redefine what one is looking for.

These items of software are sometimes called communications packages, or asynchronous comms packages, and sometimes terminal emulators, on the grounds that the software can make the micro appear to be a variety of different computer terminals. Until recently, most on-line computer services assumed that they were being examined through 'dumb' terminals--simply a keyboard and a screen, with no attendant processing or storage power (except perhaps a printer). With the arrival of PCs all this is slowly changing, so that the remote computer has to do no more than provide relatively raw data and all the formatting and on-screen presentation is done by the user's own computer. Terminal emulator software is a sort of half-way house between 'dumb' terminals and PCs with considerable local processing power.

Given the habit of manufacturers of mainframe and mini- computers to make their products as incompatible with those of their competitors as possible (to maximise their profits), many slight variants on the 'dumb' computer terminal exist--hence the availability of terminal emulators to provide, in one software package, a way of mimicking all the popular types.

Basic software to get a computer to talk through its RS232C port, and to take in data sent to it, is trivial. What the hacker needs is software that will make his computer assume a number of different personalities upon command, store data as it is collected, and print it out.

Two philosophies of presenting such software to the user exist: first, one which gives the naive user a simple menu which says, in

effect, 'press a key to connect to database' and then performs everything smoothly, without distracting menus. Such programs need an 'install' procedure, which requires some knowledge, but most 'ordinary' users never see this. Normally, this is a philosophy of software writing I very much admire: however, as a hacker you will want the precise opposite. The second approach to terminal emulator software allows you to re configure your computer as you go on--there is plenty of on-screen help in the form of menus allowing you to turn on and off local echo, set parity bits, show non-visible control codes and so on. In a typical hack, you may have only vague information about the target computer, and much of the fun is seeing how quickly you can work out what the remote computer wants to 'see' - and how to make your machine respond.

Given the numbers of popular computers on the market, and the numbers of terminal emulators for each one, it is difficult to make a series of specific recommendations. What follows there- fore, is a list of the sort of facilities you should look for:

On-line help You must be able to change the software characteristics while on-line--no separate 'install' routine. You should be able to call up 'help' menus instantly, with simple commands --while holding on to the line.

Text buffer - The received data should be capable of going into the computer's free memory automatically so that you can view it later off-line. The size of the buffer will depend on the amount of memory left after the computer has used up the space required for its operating system and the terminal software. If the terminal software includes special graphics, as in Apple Visiterm or some of the ROM packs used with the BBC, the buffer space may be relatively small. The software should tell you how much buffer space you have used and how much is left, at any time. A useful adjunct is an auto-save facility which, when the buffer becomes full, stops the stream of text from the host computer and automatically saves the buffer text to disc. A number of associated software commands should let you turn on and off the buffer store, clear it or, when off-line, view the buffer. You should also be able to print the buffer to a 'line' printer (dot-matrix or daisy wheel or thermal image). Some terminal emulators even include a simple line editor, so that you can delete or adjust the buffer before printing. (I use a terminal emulator which saves text files in a form which can be accessed by my word-processor and use that before printing out.)

Half/full Duplex (Echo On/Off) - Most remote services use an echoing protocol: this means that when the user sends a character to the host computer, the host immediately sends back the same character to the user's computer, by way of confirmation. What the user sees on his computer screen, therefore, has been generated, not locally by his direct action on the keyboard, but remotely by the host computer. (One effect of this is that there may sometimes be a perceptible delay between keystroke and display of a letter, particularly if you are using a packet-switched connection--if the telephone line is noisy, the display may appear corrupt). This echoing protocol is known as full duplex, because both the user's computer and the host

are in communication simultaneously.

However, use of full duplex/echo is not universal, and all terminal emulators allow you to switch on and off the facility. If, for example, you are talking into a half-duplex system (i.e. no echo), your screen would appear totally blank. In these circumstances, it is best if your software reproduces on the screen your keystrokes.

** Page 20

However, if you have your computer set for half-duplex and the host computer is actually operating in full duplex. each letter will appear twice--once from the keyboard and once, echoing from the host, ggiiwiinngg tthhiiss ssoorrtt ooff eeffffeecctt. Your terminal emulator needs to able to toggle between the two states.

Data Format/Parity Setting - In a typical asynchronous protocol, each character is surrounded by bits to show when it starts, when it ends, and to signify whether a checksum performed on its binary equivalent comes out even or odd. The character itself is described, typically, in 7 bits and the other bits, start, stop and parity, bringing the number up to 10. (See chapter 2.) However, this is merely one very common form, and many systems use subtle variants -- the ideal terminal emulator software will let you try out these variants while you are still on line. Typical variants should include:

Word length	Parity	No stop bits
7	Even	2
7	Odd	2
7	Even	1
7	Odd	1
8	None	2
8	None	1
8	Even	1
8	Odd	1

(NB although the ASCII character set is 7 bit, 8 bits are sometimes transmitted with a ~padding~ bit; machine code instructions for 8-bit and 16-bit machines obviously need 8-bit transmissions.)

Show Control Characters - This is a software switch to display characters not normally part of the text that is meant to be read but which nevertheless are sent by the host computer to carry out display functions, operate protocols, etc. With the switch on, you will see line feeds displayed as ^J, a back-space as ^H and so on; see Appendix IV for the usual equivalents.

Using this device properly you will be able, if you are unable to get the text stream to display properly on your screen, to work out what exactly is being sent from the host, and modify your local software accordingly.

** Page 21

Control-Show is also useful for spotting 'funnies' in passwords and log-on procedures--a common trick is to include ^H (backspace) in the middle of a log-on so that part of the full password is overwritten. (For normal reading of text, you have Control-Show switched off, as it makes normal reading difficult.)

Macros - This is the US term, now rapidly being adopted in the UK, for the preformatting of a log-on procedure, passwords etc. Typical connecting procedures to US services like The Source, CompuServe, Dow Jones etc are relatively complicated, compared with using a local hobbyist bulletin board or calling up Prestel. Typically, the user must first connect to a packet- switched service like Telenet or Tymnet (the US commercial equivalents of BT's PSS), specify an 'address' for the host required (a long string of letters and numbers) and then, when the desired service or 'host' is on line, enter password(s) to be fully admitted. The password itself may be in several parts.

The value of the 'macro' is that you can type all this junk in once and then send off the entire stream any time you wish by means of a simple command. Most terminal emulators that have this feature allow you to preformat several such macros.

From the hacker's point of view, the best type of macro facility is one that can be itself addressed and altered in software: supposing you have only part of a password: write a little routine which successively tries all the unknowns; you can then let the computer attempt penetration automatically. (You'll have to read the emulator's manual carefully to see if it has software-addressable macros: the only people who need them are hackers, and, as we have often observed, very few out-and-out hacker products exist!)

Auto-dial - Some modems contain programmable auto-diallers so that frequently-called services can be dialled from a single keyboard command.

Again the advantage to the hacker is obvious--a partly- known telephone number can be located by writing some simple software routine to test the variables.

However, not all auto-dial facilities are equally useful. Some included in US-originated communications software and terminal emulators are for specific 'smart' modems not available elsewhere--and there is no way of altering the software to work with other equipment. In general, each modem that contains an auto-dialler has its own way of requiring instructions to be sent to it. If an auto-dialling facility is important to you, check that your software is configurable to your choice of auto-dial modem.

Another hazard is that certain auto-diallers only operate on the multi-frequency tones method ('touch-tone') of dialling used in large parts of the United States and only very slowly being introduced in other countries. The system widely used in the UK is called 'pulse' dialling. Touch-tone dialling is much more rapid than pulse dialling, of course.

Finally, on the subject of US-originated software, some packages will only accept phone numbers in the standard North American format of: 3-digit area code, 3-digit local code, 4-digit subscriber code. In the UK and Europe the phone number formats vary quite considerably. Make sure that any auto-dial facility you use actually operates on your phone system.

Format Screen - Most professional on-line and time-share services assume an 80-column screen. The 'format screen' option in terminal emulators may allow you to change the regular text display on your micro to show 80 characters across by means of a graphics 'fiddle'; alternatively, it may give you a more readable display of the stream from the host by forcing line feeds at convenient intervals, just before the stream reaches the right- hand margin of the micro's 'natural' screen width.

Related to this are settings to handle the presentation of the cursor and to determine cursor movement about the screen-- normally you won't need to use these facilities, but they may help you when on-line to some odd-ball, non-standard service. Certain specific 'dumb' terminals like the VT52 (which has become something of a mainframe industry standard) use special sequences to move the cursor about the screen--useful when the operator is filling in standard forms of information.

Other settings within this category may allow you to view characters on your screen which are not part of the normal character set. The early Apples, for example, lacked lower case, presenting everything in capitals (as does the ZX81), so various ingenious 'fixes' were needed to cope. Even quite advanced home computers may lack some of the full ASCII character set, such oddities as the tilde ~ or backslash \ or curly bracket { }, for example.

Re-assign - keyboard A related problem is that home micro keyboards may not be able to generate all the required characters the remote service wishes to see. The normal way to generate an ASCII character not available from the keyboard is from Basic, by using a Print CHR$(n) type command. This may not be possible when on-line to a remote computer, where everything is needed in immediate mode. Hence the requirement for a software facility to re-assign any little-used key to send the desired 'missing' feature. Typical requirements are BREAK~ ESC, RETURN (when part of a string as opposed to being the end of a command) etc. When re-assigning a series of keys, you must make sure you don't interfere with the essential functioning of the terminal emulator.

For example, if you designate the sequence ctrl-S to mean 'send a DC1 character to the host', the chances are you will stop the host from sending anything to you, because ctrl-S is a common command (sometimes called XOF) to call for a pause--incidentally, you can end the pause by hitting ctrl-Q. Appendix IV gives a list of the full ASCII implementation and the usual 'special' codes as they apply to computer-to-computer communications.

File Protocols - When computers are sending large files to each other, a further layer of protocol, beyond that defining individual letters, is necessary. For example, if your computer is automatically saving to disk at regular intervals as the buffer fills up, it is necessary to be able to tell the host to stop sending for a period, until the save is complete. On older time-share services, where the typical terminal is a teletypewriter, the terminal is in constant danger of being unable mechanically to keep up with the host computer's output. For this reason, many host computers use one of two well-known protocols which require the regular exchange of special control characters for host and user to tell each other all is well. The two protocols are:

Stop/Start - The receiving computer can at any time send to the host a Stop (ctrl-S) signal, followed by, when it is ready a Start, (ctrl-Q).

EOB/ACK - The sending computer divides its file into a blocks (of any convenient length); after each block is sent, an EOB (End of Block) character is sent (see ASCII table, Appendix IV). The user's computer must then respond with a ACK (Acknowledge) character.

These protocols can be used individually, together or not at all. You may be able to use the 'Show Control Codes' option to check whether either of the protocols are in use. Alternatively, if you have hooked on to a service which for no apparent reason, seems to stop in its tracks, you could try ending an ACK or Start (ctrl-F or ctrl-S) and see if you can get things moving.

File transmission - All terminal emulators assume you will want to send, as well as receive, text files. Thus, in addition to the protocol settings already mentioned, there may be additional ones for that purpose, e.g. the XMODEM protocol very popular on bulletin boards. Hackers, of course, usually don't want to place files on remote computers.....

Specific terminal emulation - Some software has pre-formatted sets of characteristics to mimic popular commercial 'dumb' terminals. For example, with a ROM costing under £60 fitted to a BBC micro, you can obtain almost all of the features of DEC's VT100 terminal, which until recently was regarded as something of an industry-standard and costing just under £1000.

Other popular terminals are the VT52 and some Tektronix models, the latter for graphics display. ANSI have produced a 'standard' specification.

Baudot characters - The Baudot code, or International Telegraphic Code No 2, is the 5-bit code used in telex and telegraphy -- and in many wire-based news services. A few terminal emulators include it as an option, and it is useful if you are attempting to hack such services. Most software intended for use on radio link-ups (see Chapter 10) operates primarily in Baudot, with ASCII as an option.

Viewdata emulation - This gives you the full, or almost full,

graphics and text characters of UK-standard viewdata. Viewdata tv sets and adapters use a special character-generator chip and a few, mostly British-manufactured, micros use that chip also-- the Acorn Atom was one example. The BBC has a teletext mode which adopts the same display. But for most micros, viewdata emulation is a matter of using hi-res graphics to mimic the qualities of the real thing, or to strip out most of the graphics. Viewdata works on a screen 40 characters by 24 rows, and as some popular home micros have 'native' displays smaller than that, some considerable fiddling is necessary to get them to handle viewdata at all.

In some emulators, the option is referred to as Prestel or Micronet--they are all the same thing. Micronet-type software usually has additional facilities for fetching down telesoftware programs (see Chapter 10).

Viewdata emulators must attend not only to the graphics presentation, but also to split-speed operation: the usual speeds are 1200 receive from host, 75 transmit to host. USA users of such services may get them via a packet-switched network, in which case they will receive it either at 1200/1200 full duplex or at 300/300.

Integrated terminal emulators offering both 'ordinary' asynchronous emulation and viewdata emulation are rare: I have to use completely different and non-compatible bits of software on my own home set-up.

Modems

Every account of what a modem is and does begins with the classic explanation of the derivation of the term: let this be no exception. Modem is a contraction of modulator-demodulator.

A modem taking instructions from a computer (pin 2 on RS232C) converts the binary 0's and 1's into specific single tones, according to which 'standard' is being used. In RS232C/V24, binary 0 (ON) appears as positive volts and binary 1 (OFF) appears as negative volts.

The tones are then fed, either acoustically via the telephone mouth-piece into the telephone line, or electrically, by generating the electrical equivalent direct onto the line. This is the modulating process.

In the demodulating stage, the equipment sits on the phone line listening for occurrences of pre-selected tones (again according to whichever 'standard' is in operation) and, when it hears one, delivers a binary 0 or binary 1 in the form of positive or negative voltage pulses into pin 3 of the computer's serial port.

This explanation holds true for modems operating at up to 1200 baud; above this speed, the modem must be able to originate tones, and detect them according to phase as well, but since higher-speed working is unusual in dial-up ports--the hacker's special interest,

we can leave this matter to one side.

The modem is a relatively simple bit of kit: on the transmit side it consists of a series of oscillators acting as tone generators, and on receive has a series of narrow band-pass filters. Designers of modems must ensure that unwanted tones do not leak into the telephone line (exchanges and amplifiers used by telephone companies are sometimes remotely controlled by the injection of specific tones) and also that, on the receive side, only the distinct tones used for communications are 'interpreted' into binary 0s or 1s. The other engineering requirements are that unwanted electrical currents do not wander down the telephone cable (to the possible risk of phone company employees) or back into the user's computer.

Until relatively recently, the only UK source of low-speed modems was British Telecom. The situation is much easier now, but de-regulation of 'telephone line attachments', which include modems, is still so recent that the ordinary customer can easily become confused. Moreover, modems offering exactly the same service can vary in price by over 300%. Strictly speaking, all modems connected to the phone line should be officially approved by BT or other appropriate regulatory authority.

At 300 baud, you have the option of using direct-connect modems which are hard-wired into the telephone line, an easy enough exercise, or using an acoustic coupler in which you place the telephone hand-set. Acoustic couplers are inherently prone to interference from room-noise, but are useful for quick lash-ups and portable operation. Many acoustic couplers operate only in 'originate' mode, not in' answer'. Newer commercial direct- connect modems are cheaper than acoustic couplers.

At higher speeds acoustic coupling is not recommended, though a 75/1200 acoustic coupler produced in association with the Prestel Micronet service is not too bad, and is now exchanged on the second-hand market very cheaply indeed.

I prefer modems that have proper status lights--power on, line seized, transmit and receive indicators. Hackers need to know what is going on more than most users.

The table below shows all but two of the types of service you are likely to come across; V-designators are the world-wide 'official' names given by the CCITT; Bell-designators are the US names:

Service Designator	Speed	Duplex	Transmit 0	Transmit 1	Receive 0	Receive 1	Answer
V21 orig	300(*)	full	1180	980	1850	1650	-
V21 ans	300(*)	full	1850	1650	1180	980	2100
V23 (1)	600	half	1700	1300	1700	1300	2100
V23 (2)	1200	f/h(**)	2100	1300	2100	1300	2100
V23 back	75	f/h(**)	450	390	450	390	-
Bell 103 orig	300(*)	full	1070	1270	2025	2225	-
Bell 103 ans	300(*)	full	2025	2225	1070	1270	2225

Bell 202 1200 half 2200 1200 2200 1200 2025

(*)any speed up to 300 baud, can also include 75 and 110 baud services

(**)service can either be half-duplex at 1200 baud or asymmetrical full duplex, with 75 baud originate and 1200 baud receive (commonly used as viewdata user) or 1200 transmit and 75 receive (viewdata host)

The two exceptions are:
V22 1200 baud full duplex, two wire
Bell 212A The US equivalent
These services use phase modulation as well as tone.

British Telecom markets the UK services under the name of Datel--details are given in Appendix V.

BT's methods of connecting modems to the line are either to hard-wire the junction box (the two outer-wires are the ones you usually need)--a 4-ring plug and associated socket (type 95A) for most modems, a 5-ring plug and associated socket (type 96A) for Prestel applications (note that the fifth ring isn't used)--and, for all new equipment, a modular jack called type 600. The US also has a modular jack, but of course it is not compatible.

Modern modem design is greatly aided by a wonder chip called the AMD 7910. This contains nearly all the facilities to modulate and demodulate the tones associated with the popular speed services, both in the CCITT and Bell standards. The only omission--not always made clear in the advertisements--are services using 1200/1200 full-duplex, ie V22 and Bell 212A.

Building a modem is now largely a question of adding a few peripheral components, some switches and indicator lights, and a box. In deciding which 'world standard' modem to purchase, hackers should consider the following features:

Status lights you need to be able to see what is happening on the line.

Hardware/software switching - cheaper versions merely give you a switch on the front enabling you to change speeds, originate or answer mode and CClTT or Bell tones. More expensive ones feature firmware which allows your computer to send specially formatted instructions to change speed under program control. However, to make full use of this facility, you may need to write (or modify) your terminal emulator.

Auto-dial - a pulse dialler and associated firmware are included in some more expensive models. You should ascertain whether the auto-dialer operates on the telephone system you intend to hook the modem up to--some of the US 'smart' modems present difficulties outside the States. You will of course need software in your micro to address the firmware in the modem --and the software has to be part

of your terminal emulator, otherwise you gain nothing in convenience. However, with appropriate software, you can get your computer to try a whole bank of numbers one after the other.

D25 connector - this is the official 'approved' RS232CN24 physical connection--useful from the point-of-view of easy hook-up. A number of lower-cost models substitute alternative DIN connectors. You must be prepared to solder up your own cables to be sure of connecting up properly.

Documentation I always prefer items to be accompanied by proper instructions. Since hackers tend to want to use equipment in unorthodox ways, they should look for good documentation too.

** Page 28

Finally, a word on build-your-own modems. A number of popular electronics magazines and mail-order houses have offered modem designs. Such modems are not likely to be approved for direct connection to the public telephone network. However, most of them work. If you are uncertain of your kit-constructing skills, though. remember badly-built modems can be dangerous both to your computer and to the telephone network.

Test Equipment

Various items of useful test equipment occasionally appear on the second-hand market--via mail-order, in computer junk shops, in the flea-market section of exhibitions and via computer clubs.

It's worth searching out a cable 'break-out' box. This lets you restrap a RS232C cable without using a soldering iron--the various lines are brought out on to an accessible matrix and you use small connectors to make (or break) the links you require. It's useful if you have an 'unknown' modem, or an unusually configured computer.

Related, but much more expensive, is a RS232C/V24 analyser --this gives LED status lights for each of the important lines, so you can see what is happening.

Lastly, if you are a very rich and enthusiastic hacker, you can buy a protocol analyser. This is usually a portable device with a VDU, full keyboard, and some very clever firmware which examines the telephone line or RS232C port and carries out tests to see which of several popular datacomms protocols is in use. Hewlett Packard do a nice range. Protocol analysers will handle synchronous transmissions as well as synchronous. Cost: £1500 and up...and up.

** Page 29

CHAPTER 4

Targets

Wherever hackers gather, talk soon moves from past achievements and adventures to speculation about what new territory might be explored. It says much about the compartmentalisation of computer specialities in general and the isolation of micro- owners from mainstream activities in particular that a great deal of this discussion is like that of navigators in the days before Columbus: the charts are unreliable, full of blank spaces and confounded with myth.

In this chapter I am attempting to provide a series of notes on the main types of services potentially available on dial-up, and to give some idea of the sorts of protocols and conventions employed. The idea is to give voyagers an outline atlas of what is interesting and possible, and what is not.

On-line hosts

On-line services were the first form of electronic publishing: a series of big storage computers--and on occasion, associated dedicated networks -- act as hosts to a group of individual databases by providing not only mass data storage and the appropriate 'search language' to access it, but also the means for registering, logging and billing users. Typically, users access the on-line hosts via a phone number which links into a a public data network using packet switching (there's more on these networks in chapter 7).

The on-line business began almost by accident; large corporations and institutions involved in complicated technological developments found that their libraries simply couldn't keep track of the publication of relevant new scientific papers, and decided to maintain indices of the papers by name, author, subject-matter, and so on, on computer. One of the first of these was the armaments and aircraft company, Lockheed Corporation.

In time the scope of these indices expanded and developed and outsiders -- sub-contractors, research agencies, universities, government employees, etc were granted access. Other organisations with similar information-handling requirements asked if space could be found on the computer for their needs.

Eventually Lockheed and others recognised the beginnings of a quite separate business; in Lockheed's case it lead to the foundation of Dialogue, which today acts as host and marketing agent for almost 300 separate databases. Other on-line hosts include BRS (Bibliographic Retrieval Services), Comshare (used for sophisticated financial modelling), DataStar, Blaise (British Library) I P Sharp, and Euronet-Diane.

On-line services, particularly the older ones, are not especially user-friendly by modern standards. They were set up at a time when both core and storage memory was expensive, and the search languages tend to be abbreviated and formal. Typically they are used, not by the eventual customer for the information, but by professional

intermediaries--librarians and the like-- who have undertaken special courses. Originally on-line hosts were accessed by dumb terminals, usually teletypewriters like the Texas Whisperwriter portable with built-in acoustic modem, rather than by VDUs. Today the trend is to use 'front-end' intelligent software on an IBM PC which allows the naive user to pose his/her questions informally while offline; the software then redefines the information request into the formal language of the on-line host (the user does not witness this process) and then goes on-line via an auto-dial modem to extract the information as swiftly and efficiently as possible.

On-line services require the use of a whole series of passwords: the usual NUI and NUA for PSS (see chapter 7), another to reach the host, yet another for the specific information service required. Charges are either for connect-time or per record retrieved, or sometimes a combination.

The categories of on-line service include bibliographic, which merely indexes the existence of an article or book--you must then find a physical copy to read; and source, which contains the article or extract thereof. Full-text services not only contain the complete article or book but will, if required, search the entire text (as opposed to mere keywords) to locate the desired information. An example of this is LEXIS, a vast legal database which contains nearly all important US and English law judgements, as well as statutes.

News Services

The vast majority of news services, even today, are not, in the strictest sense, computer-based, although computers play an important role in assembling the information and, depending on the nature of the newspaper or radio or tv station receiving it, its subsequent handling.

The world's big press agencies--United Press, Associated Press, Reuters, Agence France Presse, TASS, Xinhua, PAP, VoA -- use telex techniques to broadcast their stories. Permanent leased telegraphy lines exist between agencies and customers, and the technology is pure telex: the 5-bit Baudot code (rather than ASCII) is adopted, giving capital letters only, and 'mark' and space' are sent by changing voltage conditions on the line rather than audio tones. Speeds are 50 or 75 baud.

The user cannot interrogate the agency in any way. The stories come in a single stream which is collected on rolls of paper and then used as per the contract between agency and subscriber. To hack a news agency line you will need to get physically near the appropriate leased line, tap in by means of an inductive loop, and convert the changing voltage levels (+80 volts on the line) into something your RS232C port can handle. You will then need software to translate the Baudot code into the ASCII which your computer can handle internally, and display on screen or print to a file. The Baudot code is given in Appendix IV.

None of this is easy and will probably involve breaches of several laws, including theft of copyright material! However a number of news agencies also transmit services by radio, in which case the signals can be hijacked with a short-wave receiver. Chapter 9 explains.

Historic news, as opposed to the current stuff from agencies, is now becoming available on-line. The New York Times, for example, has long held its stories in an electronic 'morgue' or clippings library. Initially this was for internal use, but for the last several years it has been sold to outsiders, chiefly broadcasting stations and large corporations. You can search for information by a combination of keyword and date-range. The New York Times Information Bank is available through several on-line hosts.

As the world's great newspapers increasingly move to electronic means of production--journalists working at VDUs, sub-editors assembling pages and direct-input into photo-typesetters--the additional cost to each newspaper of creating its own morgue is relatively slight and we can expect to see many more commercial services.

In the meantime, other publishing organisations have sought to make available articles, extract or complete, from leading magazines also. Two UK examples are Finsbury Data Services' Textline and Datasolve's d Reporter, the latter including material from the BBC's monitoring service, Associated Press, the Economist and the Guardian. Textline is an abstract service, but World Reporter gives the full text. In October 1984 it already held 500 million English words.

In the US there is NEXIS, which shares resources with LEXIS; NEXIS held 16 million full text articles at that same date. All these services are expensive for casual use and are accessed by dial-up using ordinary asynchronous protocols.

Many electronic newsrooms also have dial-in ports for reporters out on the job; depending on the system these ports not only allow the reporter to transmit his or her story from a portable computer, but may also (like Basys Newsfury used by Channel Four News) let them see news agency tapes, read headlines and send electronic mail. Such systems have been the subject of considerable hacker speculation.

Financial Services

The financial world can afford more computer aids than any other non-governmental sector. The vast potential profits that can be made by trading huge blocks of currency, securities or commodities--and the extraordinary advantages that a slight 'edge' in information can bring--have meant that the City, Wall Street and the equivalents in Hong Kong, Japan and major European capitals have been in the forefront of getting the most from high-speed comms.

Ten years ago the sole form of instant financial information was the ticker tape--telegraphy technology delivering the latest share price movements in a highly abbreviated form. As with its news

equivalents, these were broadcast services (and still are, for the services still exist) sent along leased telegraph lines. The user could only watch, and 'interrogation' consisted of back-tracking along a tape of paper. Extel (Exchange Telegraph) continues to use this technique, though it is gradually upgrading by using viewdata and intelligent terminals.

However, just over ten years ago Reuters put together the first packages which gave some intelligence and 'questioning power' to the end user. Each Reuters' Monitor is intelligent, containing (usually) a DEC PDP-8 series mini and some firmware which accepts and selects the stream of data from the host at the far end of the leased line, marshalls interrogation requests and takes care of the local display. Information is formatted in 'pages' rather like viewdata frames, but without the colour. There is little point in eavesdropping into a Reuters line unless you know what the terminal firmware does. Reuters now face an aggressive rival in Telerate, and the fight is on to deliver not only fast comprehensive prices services but international screen-based dealing as well. The growth of Reuters and its rivals is an illustration of technology creating markets--especially in international currency--where none existed before.

** Page 33

The first sophisticated Stock Exchange prices 'screens' used modified closed circuit television technology. London had a system called Market Price Display Service--MPDS--which consisted of a number of tv displays of current prices services on different 'channels' which could be selected by the user. But London now uses TOPIC, a leased line variant on viewdata technology, though with its magazine-like arrangement and auto-screen refresh, it has as much in common with teletext as Prestel. TOPIC carries about 2,500 of the total 7,500 shares traded in London, plus selected analytical material from brokers. Datastream represents a much higher level of sophistication: using its £40,000 plus pa terminals you can compare historic data-- price movements, movements against sector indices etc--and chart the results.

The hacker's reward for getting into such systems is that you can see share and other prices on the move. None of these prices is confidential; all could be obtained by ringing a stockbroker. However, this situation is likely to change; as the City makes the change from the traditional broker/jobber method of dealing towards specialist market making, there will then be electronic prices services giving privileged information to specialist share dealers. All these services are only available via leased lines; City professionals would not tolerate the delays and uncertainties of dial-up facilities. However dial-up ports exist for demonstrations, exhibitions, engineering and as back-up--and a lot of hacking effort has gone into tracking them down.

In the United States, in addition to Reuters, Telerate and local equivalents of official streams of stock exchange and over-the-counter data, there is Dow Jones, best known internationally for its market indices similar to those produced by the Financial Times in London. Dow Jones is in fact the owner of the Wall Street Journal and some influential business magazines. Its Dow Jones News/Retrieval

Service is aimed at businesses and private investors. It features current share prices, deliberately delayed by 15 minutes, historic price data, which can be charted by the user's own computer (typically an Apple or IBM PC) and historic 'morgue' type company news and analysis. Extensions of the service enable customers to examine accounts of companies in which they are interested. The bulk of the information is US-based, but can be obtained world-wide via packet-switching networks. All you need are the passwords and special software.

** Page 34

Business Information

Business information is usually about the credit-worthiness of companies, company annual reports, trading opportunities and market research. The biggest electronic credit data resource is owned by the international company Dun & Bradstreet: during 1985-86 it is due to spend £25m on making its data available all over Europe, including the UK. The service, which covers more than 250,000 UK businesses, is called DunsPrint and access is both on-line and via a viewdata front-end processor. Another credit agency, CNN Services, extensively used already by the big clearing banks, and with 3000 customers accessing information via viewdata sets, has recently also announced an extended electronic retrieval service for its own called Guardian Business Information A third UK credit service available electronically is called InfoLink.

In addition, all UK companies quoted on the London Stock Exchange and many others of any size who are not, have a report and analysis available from ICC (InterCompany Comparisons) who can be accessed via on--line dial--up, through a viewdata interface and also by Datastream customers. Dun & Bradstreet also have an on--line service called KBE covering 20,000 key British enterprises.

Prodigious quantities of credit and background data on US companies can be found on several of the major on--line hosts. A valid phone number, passwords and extracts from the operations manual of one of the largest US services, TRW--it has credit histories on 90 million people--sat on some hackers' bulletin boards (of which much more later) for over twelve months during 1983 and 1984 before the company found out. No one knows how many times hackers accessed the service. According to the Washington Post, the password and manual had been obtained from a Sears Roebuck national chain store in Sacramento; some hackers claimed they were able to alter credit records, but TRW maintain that telephone access to their systems is designed for read-only operations alone, updating of files taking place solely on magnetic tape.

US market research and risk analysis comes from Frost Sullivan. Risk analysis tells international businessmen which countries are politically or economically unstable, or likely t become so, and so unsafe to do business with. I once found myself accessing a viewdata-based international assessment service run b a company called Control Risks, which reputedly has strong link to the Special Air Service. As so often happens when hacker think they are about to

uncover secret knowledge, the actual data files seemed relatively trivial, the sort of judgements that could be made by a bright sixth former who read posh newspapers and thoughtful weekly magazines.

** Page 35

University facilities

In complete contrast to computers that are used to store and present data are those where the value is to deliver processing power to the outside world. Paramount among these are those installed in universities and research institutes.

Although hackers frequently acquire phone numbers to enter such machines, what you can do once you are there varies enormously. There are usually tiers and banks of passwords, each allowing only limited access to the range of services. It takes considerable knowledge of the machine's operating system to break through from one to another and indeed, in some cases, the operating system is so thoroughly embedded in the mainframe's hardware architecture that the substantial modifications necessary to permit a hacker to roam free can only be done from a few designated terminals, or by having physical access to the machine. However, the hobbyist bulletin board system quite often provides passwords giving access to games and the ability to write and run programs in exotic languages--my own first hands--on experience of Unix came in exactly this way. There are bulletin boards on mainframes and even, in some cases, boards for hackers!

Given the nature of hacking, it is not surprising that some of the earliest japes occurred on computers owned by universities. Way back in the 1970s, MIT was the location of the famous 'Cookie Monster', inspired by a character in the then-popular Rowan & Martin Laugh-in television show. As someone worked away at their terminal, the word 'cookie' would appear across their screen, at first slowly wiping out the user's work. Unless the user moved quickly, things started to speed up and the machine would flash urgently: "Cookie, cookie, give me a cookie". The whole screen would pulse with this message until, after a while, the hacking program relented and the 'Monster' would clear the screen, leaving the message: "I didn't want a cookie anyway." It would then disappear into the computer until it snared another unsuspecting user. You could save yourself from the Monster by typing the word "Cookie", to which it replied "Thank you" and then vanished.

In another US case, this time in 1980, two kids in Chicago, calling themselves System Cruncher and Vladimir, entered the computer at DePaul University and caused a system crash which cost $22,000 to fix. They were prosecuted, given probation and were then made a movie offer.

** Page 36

In the UK, many important university and research institution computers have been linked together on a special data network called SERCNET. SERC is the Science and Engineering Research Council.

Although most of the computers are individually accessible via PSS, SERCNET makes it possible to enter one computer and pass through to others. During early 1984, SERCNET was the target of much hacker attention; a fuller account appears in chapter 7, but to anticipate a little, a local entry node was discovered via one of the London University college computers with a demonstration facility which, if asked nicely, disgorged an operating manual and list of 'addresses'. One of the minor joys of this list was an entry labelled "Gateway to the Universe", pure Hitch-hiker material, concealing an extensive long-term multi-function communications project. Eventually some hackers based at a home counties university managed to discover ways of roaming free around the network....

Banking

Prominent among public fantasies about hackers is the one where banks are entered electronically, accounts examined and some money moved from one to another. The fantasies, bolstered by under-researched low-budget movies and tv features, arise from confusing the details of several actual happenings.

Most 'remote stealing' from banks or illicit obtaining of account details touch computers only incidentally and involve straight-forward fraud, conning or bribery of bank employees. In fact, when you think about the effort involved, human methods would be much more cost-effective for the criminal. For hackers, however, the very considerable effort that has been made to provide security makes the systems a great challenge in them- selves.

In the United Kingdom, the banking scene is dominated by a handful of large companies with many branches. Cheque clearing and account maintenance are conducted under conditions of high security with considerable isolation of key elements; inter-bank transactions in the UK go through a scheme called CHAPS, Clearing House Automatic Payments System, which uses the X.25 packet switching protocols (see chapter 7). The network is based on Tandem machines; half of each machine is common to the network and half unique to the bank. The encryption standard used is the US Data Encryption Standard. Certain parts of the network, relating to the en- and de-cryption of messages, apparently auto-destruct if tampered with.

The service started early in 1984. The international equivalent is SWIFT (Society for Worldwide Interbank Financial Transactions); this is also X.25- based and it handles about half-a-million messages a day. If you want to learn someone's balance, the easiest and most reliable way to obtain it is with a plausible call to the local branch. If you want some easy money, steal a cheque book and cheque card and practise signature imitation. Or, on a grander scale, follow the example of the £780,000 kruggerand fraud in the City. Thieves intercepted a telephone call from a solicitor or bank manager to 'authenticate' forged drafts; the gold coins were then delivered to a bogus company.

In the United States, where federal law limits the size of an

individual bank's operations and in international banking, direct attacks on banks has been much easier because the technology adopted is much cruder and more use is made of public phone and telex lines. One of the favourite techniques has been to send fake authorisations for money transfers. This was the approach used against the Security National Pacific Bank by Stanley Rifkin and a Russian diamond dealer in Geneva. $10.2m moved from bank to bank across the United States and beyond. Rifkin obtained code numbers used in the bilateral Test Keys. The trick is to spot weaknesses in the cryptographic systems used in such authorisations. The specifications for the systems themselves are openly published; one computer security expert, Leslie Goldberg, was recently able to take apart one scheme--proposed but not actually implemented--and show that much of the 'key' that was supposed to give high level cryptographic security was technically redundant, and could be virtually ignored. A surprisingly full account of his 'perfect' fraud appears in a 1980 issue of the journal Computer Fraud and Security Bulletin.

There are, however, a few areas where banking is becoming vulnerable to the less mathematically literate hacker. A number of international banks are offering their big corporation customers special facilities so that their Treasury Departments (which ensure, among other things, that any spare million dollars are not left doing nothing over night but are earning short-term interest) can have direct access to their account details via a PC on dial-up. Again, telebanking is now available via Prestel and some of its overseas imitators. Although such services use several layers of passwords to validate transactions, if those passwords are mis-acquired, since no signatures are involved, the bank account becomes vulnerable.

Finally, the network of ATMs (hole-in-the-wall cash machines) is expanding greatly. As mentioned early in this book, hackers have identified a number of bugs in the machines. None of them, incidentally, lead directly to fraud. These machines allow card-holders to extract cash up to a finite limit each week (usually £100). The magnetic stripe contains the account number, validation details of the owner's PIN (Personal Identity Number), usually 4 digits, and a record of how much cash has been drawn that week. The ATM is usually off-line to the bank's main computer and only goes on-line in two circumstances--first, during business hours, to respond to a customer's 'balance request'; and second, outside regular hours, to take into local memory lists of invalid cards which should not be returned to the customer, and to dump out cheque book and printed statement requests.

Hackers have found ways of getting more than their cash limit each week. The ATMs belonging to one clearing bank could be 'cheated' in this way: you asked for your maximum amount and then, when the transaction was almost completed, the ATM asked you 'Do you want another transaction, Yes/No?' If you responded 'yes' you could then ask for--and get--your credit limit again, and again, and again. The weakness in the system was that the magnetic stripe was not overwritten to show you had had a transaction till it was physically ejected from the machine. This bug has now been fixed.

A related but more bizarre bug resided for a while on the ATMs used by that first bank's most obvious High Street rivals. In that case, you had to first exhaust your week's limit. You then asked for a further sum, say £75. The machine refused but asked if you wanted a further transaction. Then, you slowly decremented the amounts you were asking for by £5...70, 65, 60...and so on, down to £10. You then told the ATM to cancel the last £5 transaction...and the machine gave you the full £75. Some hackers firmly believe the bug was placed there by the original software writer. This bug too has now been fixed.

Neither of these quirks resulted in hackers 'winning' money from the banks involved; the accounts were in every case, properly debited. The only victory was to beat the system. For the future, I note that the cost of magnetic stripe reader/writers which interface to PCs is dropping to very low levels. I await the first inevitable news reports.

Electronic Mail

Electronic mail services work by storing messages created by some users until they are retrieved by their intended recipients.

The ingredients of a typical system are: registration/logging on facilities, storage, search and retrieval, networking, timing and billing. Electronic mail is an easy add-on to most mainframe installations, but in recent years various organisations have sought to market services to individuals, companies and industries where electronic mail was the main purpose of the system, not an add-on.

The system software in widest use is that of ITI-Dialcom; it's the one that runs Telecom Gold. Another successful package is that used in the UK and USA by Easylink, which is supported by Cable & Wireless and Western Union.

In the Dialcom/Telecom Gold service, the assumption is made that most users will want to concentrate on a relatively narrow range of correspondents. Accordingly, the way it is sold is as a series of systems, each run by a 'manager': someone within a company. The 'manager' is the only person who has direct contact with the electronic mail owner and he in turn is responsible for bringing individual users on to his 'system' -- he can issue 'mailboxes' direct, determine tariff levels, put up general messages. In most other services, every user has a direct relationship with the electronic mail company.

The services vary according to their tariff structures and levels; and also in the additional facilities: some offer bi-directional interfaces to telex; and some contain electronic magazines, a little like videotex.

The basic systems tend to be quite robust and hacking is mainly concentrated on second-guessing users IDs. Many of the systems have now sought to increase security by insisting on passwords of a

certain length--and by giving users only three or four attempts at logging on before closing down the line. But increasingly their customers are using PCs and special software to automate logging-in. The software packages of course have the IDs nicely pre-stored....

Government computers

Among hackers themselves the richest source of fantasising revolves around official computers like those used by the tax and national insurance authorities, the police, armed forces and intelligence agencies.

The Pentagon was hacked in 1983 by a 19-year-old Los Angeles student, Ronald Austin. Because of the techniques he used, a full account is given in the operating systems section of chapter 6. NASA, the Space Agency, has also acknowledged that its e-mail system has been breached and that messages and pictures of Kilroy were left as graffiti.

** Page 40

This leaves only one outstanding mega-target, Platform, the global data network of 52 separate systems focused on the headquarters of the US's electronic spooks, the National Security Agency at Fort Meade, Maryland. The network includes at least one Cray-1, the worlds most powerful number-cruncher, and facilities provided by GCHQ at Cheltenham.

Although I know UK phone freaks who claim to have managed to appear on the internal exchanges used by Century House (M16) and Curzon Street House (M15) and have wandered along AUTOVON, the US secure military phone network, I am not aware of anyone bold or clever enough to have penetrated the UK's most secure computers.

It must be acknowledged that in general it is far easier to obtain the information held on these machines--and lesser ones like the DVLC (vehicle licensing) and PNC (Police National Computer)-- by criminal means than by hacking -- bribery, trickery or blackmail, for example. Nevertheless, there is an interesting hacker's exercise in demonstrating how far it is possible to produce details from open sources of these systems, even when the details are supposed to be secret. But this relates to one of the hacker's own secret weapons--thorough research, the subject of the next chapter.

** Page 41

CHAPTER 5

Hackers' Intelligence

Of all the features of hacking that mystify outsiders, the first is how the hackers get the phone numbers that give access to the computer systems, and the passwords that open the data. Of all the

ways in which hacking is portrayed in films, books and tv, the most misleading is the concentration on the image of the solitary genius bashing away at a keyboard trying to 'break in'.

It is now time to reveal one of the dirty secrets of hacking: there are really two sorts of hacker. For this purpose I will call them the trivial and the dedicated. Anyone can become a trivial hacker: you acquire, from someone else, a phone number and a password to a system; you dial up, wait for the whistle, tap out the password, browse around for a few minutes and log off. You've had some fun, perhaps, but you haven't really done anything except follow a well-marked path. Most unauthorised computer invasions are actually of this sort.

The dedicated hacker, by contrast, makes his or her own discoveries, or builds on those of other pioneers. The motto of dedicated hackers is modified directly from a celebrated split infinitive: to boldly pass where no man has hacked before.

Successful hacking depends on good research. The materials of research are all around: as well as direct hacker-oriented material of the sort found on bulletin board systems and heard in quiet corners during refreshment breaks at computer clubs, huge quantities of useful literature are published daily by the marketing departments of computer companies and given away to all comers: sheaves of stationery and lorry loads of internal documentation containing important clues are left around to be picked up. It is up to the hacker to recognise this treasure for what it is, and to assemble it in a form in which it can be used.

Anyone who has ever done any intelligence work, not necessarily for a government, but for a company, or who has worked as an investigative journalist, will tell you that easily 90% of the information you want is freely available and that the difficult part is recognising and analysing it. Of the remaining 10%, well over half can usually be inferred from the material you already have, because, given a desired objective, there are usually only a limited number of sensible solutions.

You can go further: it is often possible to test your inferences and, having done that, develop further hypotheses. So the dedicated hacker, far from spending all the time staring at a VDU and 'trying things' on the keyboard, is often to be found wandering around exhibitions, attending demonstrations, picking up literature, talking on the phone (voice-mode!) and scavenging in refuse bins.

But for both trivial operator, and the dedicated hacker who wishes to consult with his colleagues, the bulletin board movement has been the single greatest source of intelligence.

Bulletin Boards

Since 1980, when good software enabling solitary micro-computers to offer a welcome to all callers first became widely available, the

bulletin board movement has grown by leaps and bounds. If you haven t logged on to at least one already, now is the time to try. At the very least it will test out your computer, modem and software --and your skills in handling them. Current phone numbers, together with system hours and comms protocol requirements, are regularly published in computer mags; once you have got into one, you will usually find current details of most of the others.

Somewhere on most boards you will find a series of Special Interest Group (SIG) sections and among these, often, will be a Hacker's Club. Entrance to each SIG will be at the discretion of the Sysop, the Bulletin Board owner. Since the BBS software allows the Sysop to conceal from users the list of possible SIGs, it may not be immediately obvious whether a Hacker's section exists on a particular board. Often the Sysop will be anxious to form a view of a new entrant before admitting him or her to a 'sensitive' area. It has even been known for bulletin boards to carry two hacker sections: one, admission to which can be fairly easily obtained; and a second, the very existence of which is a tightly-controlled secret, where mutually trusting initiates swap information.

The first timer, reading through a hacker's bulletin board, will find that it seems to consist of a series of discursive conversations between friends. Occasionally, someone may write up a summary for more universal consumption. You will see questions being posed. if you feel you can contribute, do so, because the whole idea is that a BBS is an information exchange. It is considered crass to appear on a board and simply ask 'Got any good numbers?; if you do, you will not get any answers. Any questions you ask should be highly specific, show that you have already done some ground-work, and make clear that any results derived from the help you receive will be reported back to the board.

Confidential notes to individuals, not for general consumption, can be sent using the E-Mail option on the bulletin board, but remember, nothing is hidden from the Sysop.

A flavour of the type of material that can be seen on bulletin boards appears from this slightly doctored excerpt (I have removed some of the menu sequences in which the system asks what you want to do next and have deleted the identities of individuals):

Msg#: 3538 *Modem Spot*
01/30/84 12:34:54 (Read 39 Times)
From: xxxxxxxxxx
To: ALL
Subj: BBC/MAPLIN MODEMS
RE THE CONNECTIONS ON THE BBC/MAPLIN MODEM SETUP. THE crs PIN IS USED TO HANDSHAKE WITH THE RTS PIN E.G. ONE UNIT SENDS RTS (READY TO SEND) AND SECOND UNIT REPLIES CTS (CLEAR TO SEND). USUALLY DONE BY TAKING PIN HIGH. IF YOU STRAP IT HIGH I WOULD SUGGEST VIA A 4K7 RESISTOR TO THE VCC/+VE RAIL (5V). IN THE EVENT OF A BUFFER OVERFLOW THESE RTS/CTS PINS ARE TAKEN LOW AND THIS STOPS THE DATA TRANSFER. ON A 25WAY D TYPE CONNECTOR TX DATA IS PIN 2
RX DATA IS PIN 3
RTS IS PIN 4

CTS IS PIN 5
GROUND IS PIN 7

ALL THE BEST -- ANY COMMTO XXXXXXXXX
(DATA COMMS ENGINEER)

Msg#: 3570 *Modem Spot*
01/31/84 23:43:08 (Read 31 Times)
From: XXXXXXXXXX
To: XXXXXXXXXX
Subj: REPLY TO MSG# 3538 (BBC/MAPLIN MODEMS)
ON THE BBC COMPUTER IT IS EASIER TO CONNECT THE RTS (READY TO SEND) PIN HE CTS (CLEAR TO SEND) PIN. THIS OVERCOMES THE PROBLEM OF HANDSHAKING.
SINCE THE MAPLIN MODEM DOES NOT HAVE HANDSHAKING.I HAVE PUT MY RTS CTS JUMPER INSIDE THE MODEM. MY CABLES ARE THEN STANDARD AND CAN BE USED WITH HANDSHAKERS.
REGARDS

Hsg#: 3662 *HACKER'S CLUB*
02/04/84 23:37:11 (Read 41 Times)
From: XXXXXXXXXX
To: ALL
Subj: PUBLIC DATA NET
Does anyone know what the Public Data Net is? I appear to have access to it, & I daren't ask what it is!
Also, can anyone tell me more about the Primenet systems... Again I seem to have the means,but no info. For instance, I have a relative who logs on to another Prime Both of our systems are on Primenet, is there any way we can communicate?
More info to those who want it...

<N>ext msg, <R>eply, or <S>top?
Msg has replies, read now(Y/N)? y

Reply has been deleted

<N>ext msg, <R>eply, or <S>top?

Msg#: 3739 *HACKER'S CLUB*
02/06/84 22:39:06 (Read 15 Times)
From: xxxxxxxxxx
To: xxxxxxxxxx
Subj: REPLY TO MSG# 3716 (PRIMENET COMMS)
Ahh, but what is the significance of the Address-does it mean a PSS number. or some thing like that? Meanwhile, I'II get on-line (via voice-link on the phone!) to my cousin, and see what he has on it....

Msg#: 3766 *HACKER'S CLUB*
02/07/84 13:37:54 (Read 13 Times)
From: xxxxxxxxxxx
To: xxxxxxxxxxx
Subj: REPLY TO MSG# 3751 (PUBLIC DATA NET)
Primenet is a local network. I know of one in Poole, An BTGold use one between their systems too. It Is only an internal network, I suggest using PSS to communicate between different primes. Cheers.

<N>ext msg, <R>eply, or <S>top?

Msg#: 3799 *BBC*
02/07/84 22:09:05 (Read 4 Times)
From: xxxxxxxxxxx
To: xxxxxxxxxxx
Subj: REPLY TO MSG# 3751 (RGB VIDEO)
The normal video output BNC can be made to produce colour video by making a link near to the bnc socket on the pcb. details are in the advanced user guide under the chapter on what the various links do. If you require more I will try to help, as I have done this mod and it works fine

Msg#: 935 *EREWHON*
09/25/83 01:23:00 (Read 90 Times)
From: xxxxxxxxxx
To: ALL
Subj: US PHONE FREAKING
USA Phone Freaking is done with a 2 out of 5 Code. The tones must be with 30Hz, and have less than 1% Distortion.

Master Tone Frequency = 2600 Hz.
>1 = 700 & 900 Hz
>2 = 700 & 1100 Hz
>3 = 900 & 1100 HZ
>4 = 700 & 1300 Hz
>5 = 900 & 1300 Hz
>6 = 1100 & 1300 Hz
>7 = 700 & 1500 HZ
>8 = 900 & 1500 Hz
>9 = 1100 & 1500 Hz
>0 = 1300 & 1500 Hz
>Start Key Signal = 1100 & 1700 Hz
>End Key Signal = 1300 & 1700 Hz
> Military Priority Keys 11=700 & 1700 ; 12=900 & 1700 - I don't recommend using these. (The method of use will be explained in a separate note. DO NOT DISCLOSE WHERE YOU GOT THESE FREQUENCIES TO ANYONE!

Msg#: 936 *EREWHON*
09/20/83 01:34:43 (Read 89 Times)
From: xxxxxxxxxxxx
To: ALL
Subj: UK PHONE FREAKING

The UK System also uses a 2 out of 5 tone pattern.

The Master Frequency is 2280 Hz
>I = 1380 & 1500 Hz
>2 = 1380 & 1620 Hz
>3 = 1500 & 1620 Hz
>4 = 1380 & 1740 Hz
>5 = 1500 & 1740 Hz
>6 = 1620 & 1740 Hz
>7 = 1380 & I860 Hz
>8 = 1500 & 1860 Hz
>9 = 1620 & 1860 Hz

>0 = 1740 & 1860 Hz
>Start Key = 1740 & 1980 ; End Keying = 1860 & 1980 Hz
>Unused I think 11 = 1380 & 1980 ; 12 = 1500 & 1980 Hz

This is from the CCITT White Book Vol. 6 and is known as SSMF No. 3 to some B.T. Personnel.

The 2280 Hz tone is being filtered out at many exchanges so you may need quite high level for it to work.

** Page 45

Msg#: 951 *EREWHON*
09/21/83 17:44:28 (Read 79 Times)
From: xxxxxxxxxx
To: PHONE FREAK's
Subj: NEED YOU ASK ?
In two other messages you will find the frequencies listed for the Internal phone system controls. This note is intended to explain how the system could be operated. The central feature to realise is that (especially in the (USA) the routing information in a call is not in the Dialled Code. The normal sequence of a call is that the Area Code is received while the Subscriber No. Is stored for a short period. The Local Exchange reads the area code and selects the best route at that time for the call. The call together with a new "INTERNAL" dialling code Is then sent on to the next exchange together with the subscriber number. This is repeated from area to area and group to group. The system this way provides many routes and corrects itself for failures.

The Technique. make a Long Distance call to a number which does not answer. Send down the Master Tone. (2600 or 22080 Hz) This will clear the line back, but leave you in the system. You may now send the "Start key Pulse" followed by the Routing Code and the Subscriber No. Finish with the "End keying Pulse". The system sees you as being a distant exchange requesting a route for a call.

Meanwhile back at the home base. Your local exchange will be logging you in as still ringing on the first call. There are further problems in this in both the USA and the UK as the techniques are understood and disapproved of by those in authority. You may need to have a fairly strong signal into the system to get past filters present on the line. Warning newer exchanges may link these filters to alarms. Try from a phone box or a Public Place and see what happens or who comes.

Example:- To call from within USA to Uk:
> Ring Toll Free 800 Number
> Send 2600 Hz Key Pulse
> When line goes dead you are in trunk level
> Start Pulse 182 End Pulse = White Plains N.Y. Gateway continued in next message

Hsg#: 952 *EREWHON*
09/21/83 18:03:12 (Read 73 Times)
From: xxxxxxxxxx
To: PHONE FREAKS

Subj: HOW TO DO IT PT 2

> Start Pulse 044 = United Kingdom
> 1 = London (Note no leading O please)
> 730 1234 = Harrods Department Store.

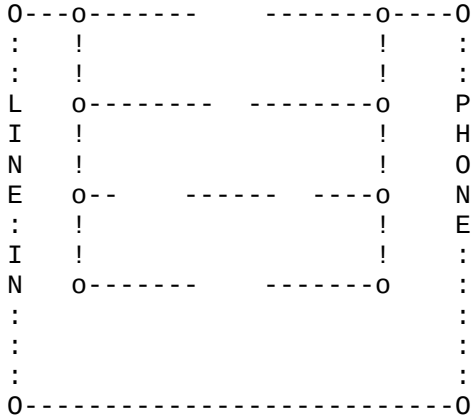
Any info on internal address codes would be appreciated from any callers.

Msg#: 1028 *EREWHON*
09/25/83 23:02:35 (Read 94 Times)
From: xxxxxxxxxxx
To: ALL
Subj: FREEFONE PART I

The following info comes from a leaflet entitled 'FREEFONE':

"British Telecom's recent record profits and continuing appalling service have prompted the circulation of this information. It comprises a method of making telephone calls free of charge."

Circuit Diagram:



** Page 46

S1 = XXX
C1 = XXX
D1 = XXX
D2 = XXX
R1 = XXX

Continued...

MSG#: 1029 *EREWHON*
09/25/83 23:19:17 (Read 87 Times)
From xxxxxxxxxx
To: ALL
Subj: FREEFONE PART 2

Circuit Operation:

The circuit inhibits the charging for incoming calls only. When a

phone is answered, there is normally approx. IOOmA DC loop current but only 8mA or so is necessary to polarise the mic In the handset. Drawing only this small amount is sufficient to fool BT's ancient "Electric Meccano".

It's extremely simple. When ringing, the polarity of the line reverses so D1 effectively answers the call when the handset is lifted. When the call is established, the line polarity reverts and R1 limits the loop current while D2 is a LED to indicate the circuit is in operation. C1 ensures speech is unaffected. S1 returns the telephone to normal.

Local calls of unlimited length can be made free of charge. Long distance calls using this circuit are prone to automatic disconnection this varies from area to area but you will get at least 3 minutes before the line is closed down. Further experimentation should bear fruit in this respect.

Sith the phone on the hook this circuit is completely undetectable. The switch should be cLosed if a call is received from an operator, for example, or to make an outgoing call. It has proved extremely useful, particularly for friends phoning from pay phones with jammed coin slots.

Please DO NOT tell ANYONE where yoU found this information

Msg#: 1194 *EREWHON*
10/07/83 04:50:34 (Read 81 Times)
From: xxxxxxxxxxxx
To: ALL
Subj: FREE TEST NUMBERS

Free Test Numbers

Here are some no's that have been found to work:
Dial 174 <last 4 figs of your no>: this gives unobtainable then when you replace handset the phone rings.

Dial 175 <last 4 figs of your no: this gives 'start test...start test...', then when you hang-up the phone rings. Pick it up and you either get dial tone which indicates OK or you will get a recording i.e 'poor insulation B line' telling you what's wrong. If you get dial tone you can immediately dial 1305 to do a further test which might say 'faulty dial pulses'. Other numbers to try are 182, 184 or 185. I have discovered my exchange (Pontybodkin) gives a test ring for 1267. These numbers all depend on you local exchange so It pays to experiment, try numbers starting with 1 as these are all local functions. Then when you discover something of interest let me know on this SIG.

Msg: 2241 *EREWHON*
12/04/83 20:48:49 (Read 65 Times)
From: SYSOP
To: SERIOUS FREAKS
Subj: USA INFO

There is a company (?) in the USA called Loopmaniacs Unlimited, PO Box 1197, Port Townsend. WA, 98368, who publish a line of books on telephone hacking. Some have circuits even. Write to M. Hoy there.

One of their publications is "Steal This Book" at S5.95 plus about $4 post. Its Worth stealing, but don't show it to the customs!

** Page 47

Msg#: 3266 *EREWHON*
01/22/84 06:25:01 (Read 53 Times)
From: xxxxxxxxxx
To: ALL
Subj: UNIVERSITY COMPUTERS
As already described getting onto the UCL PAD allows various calls. Via this network you can access many many university/research computers To get a full list use CALL 40 then HELP, select GUIDE. Typing '32' at the VIEW prompt will start listing the addresses. Host of these can be used at the pad by 'CALL addr' where addr is the address. For passwords you try DEMO HELP etc. If you find anything interesting report it here.
HINT: To aviod the PAD hanging up at the end of each call use the LOGON command - use anything for name and pwd. This seems to do the trick.
Another number: Tel: (0235) 834531. This is another data exchange. This one's a bit harder to wake up. You must send a 'break level' to start. This can be done using software but with a maplin just momentarily pull out the RS232 com. Then send RETURNs. To get a list of 'classes' you could use say Manchesters HELP:- CALL 1020300, user:DEMO pwd:DEMO en when you're on HELP PACX.

Msg#: 3687 *HACKER'S CLUB*
02/05/84 14:41:43 (Read 416 Times)
From: xxxxxxxxxxxx
To: ALL
Subj: HACKERS NUMBERS

The following are some of the numbers collected in the Hackers SIG:

Commodore BBS (Finland)   358 61 116223

Gateway test   01 600 1261
PRESTEST (1200/75)   01 583 9412
Some useful PRESTEL nodes - 640..Res.D (Martlesham's experiments in Dynamic Prestel DRCS, CEPT standards, Picture Prestel, 601 (Mailbox,Telemessaging, Telex Link - and maybe Telecom Gold), 651 (Scratchpad -always changing). Occasionally parts of 650 (IP News) are not properly CUGed off. 190 sometimes is interesting well.

These boards all specialised in lonely hearts services !
The boards with an asterisk all use BELL Tones
*Fairbanks, AK,   907-479-0315
*Burbank, CA,   213-840-8252
*Burbank, CA,   213-842-9452
*Clovis, CA,   209-298-1328
*Glendale, CA,   213-242-l882
*La Palma, CA,   714-220-0239

*Hollywood, CA,   213-764-8000
*San Francisco CA, 415-467-2588
*Santa Monica CA, 213-390-3239
*Sherman Oaks CA, 213-990-6830
*Tar~ana , CA,   213-345-1047
*Crystal Rivers FL,904-795-8850
*Atlanta, GA,   912-233-0863
*Hammond, IN,   219-845-4200
*Cleveland, OH,   216-932-9845
*Lynnefield, MA,   6l7-334-6369
*Omaha, NE,   402-571-8942
*Freehold, NJ,   201-462-0435
*New York, NY,   212-541-5975
*Cary, NC,   919-362-0676
*Newport News,VA   804-838-3973
*Vancouver, WA,   200-250-6624
Marseilles, France 33-91-91-0060

Both USA nos. prefix (0101)
a) Daily X-rated Doke Service 516-922-9463
b) Auto-Biographies of young ladies who normally work in
unpublishable magazines on 212-976-2727.
c)Dial a wank 0101,212,976,2626; 0101,212,976,2727

** Page 48

Msg#: 3688 *HACKER'S CLUB*
02/05/84 14:44:51 (Read 393 Times)
From: xxxxxxxxxxx
To: ALL
Subj: HACKERS NUMBERS CONT...
Hertford PDP 11/70 Hackers BBS:
Call 0707-263577 with 110 baud selected.
type: SET SPEED 300'CR'
After hitting CR switch to 300 baud.
Then type: HELLO 124,4'CR
!Password: HAE4 <CR>
When logged on type: COMMAND HACKER <CR>
Use: BYE to log out
****
EUCLID   388-2333
TYPE A COUPLE OF <CR> THEN PAD <CR>
ONCE LOGGED ON TO PAD TYPE CALL 40 <CR> TRY DEMO AS A USERID WHY NOT
TRY A FEW DIFFER DIFFERENT CALLS THIS WILL LET U LOG ON TO A WHOLE
NETWORK SYSTEM ALL OVER EUROPE!
YOU CAN ALSO USE 01-278-4355.
****
unknown 300 Baud   01-854 2411
01-854 2499
******
Honeywell:From London dial the 75, else 0753(SLOUGH)
75 74199 75 76930
Type- TSS
User id: D01003
password: Unknown (up to 10 chars long)
Type: EXPL GAMES LIST to list games
To run a game type: FRN GAMES(NAME) E for a fotran game.

Replace FRN with BRN for BASIC games.
******
Central London Poly 01 637 7732/3/4/5
******
PSS (300)   0753 6141
******
Comshare (300)   01 351 2311
******
'Money Box'   01 828 9090
******
Imperial College 01 581 1366
01 581 1444
****
These are most of the interesting numbers that have come up over the last bit. If I have omitted any, please leave them in a message.

Cheers, xxxxx.

Msg#: 5156 *HACKER'S CLUB*
04/15/84 08:01:11 (Read 221 Times)
From: xxxxxxxxxx
To: ALL
Subj: FINANCIAL DATABASES
You can get into Datastream on dial-up at 300/300 on 251 6180 - no I don't have any passwords....you can get into Inter Company Comparisons (ICC) company database of 60,000 companies via their 1200/75 viewdata front-end processor on 253 8788. Type ***# when asked for your company code to see a demo...

Msg#: 5195 *HACKER'S CLUB*
04/17/84 02:28:10 (Read 229 Times)
From: xxxxxxxxxx
To: ALL
Subj: PSS TELEX
THIS IS PROBOBLY OLD HAT BY NOW BUT IF YOU USE PSS THEN A92348******
WHERE **=UK TELEX NO. USE CTRL/P CLR TO BET OUT AFTER MESSAGE. YOU WILL BE CHARGED FOR USE I GUESS

Msg#: 7468 *EREWHON*
06/29/84 23:30:24 (Read 27 Times)
From: xxxxxxxxxx
To: PHREAKS
Subj: NEW(OLD..) INFO
TODAY I WAS LUCKY ENOUGH TO DISCOVER A PREVIOUSLY UNKNOWN CACHE OF AMERICAN MAGAZINE KNOWN AS TAP. ALTHOUGH THEYRE RATHER OUT OF DATE (1974-1981) OR SO THEY ARE PRETTY FUNNY AND HAVE A FEW INTERESTING BITS OF INFORMATION, ESPECIALLY IF U WANT TO SEE THE CIRCUIT DIAGRAMS OF UNTOLD AMOUNTS OF BLUE/RED/BLACK/??? BOXES THERE ARE EVEN A FEW SECTIONS ON THE UK (BUT AS I SAID ITS COMPLETELY OUT OF DATE). IN THE FUTURE I WILL POST SOME OF THE GOOD STUFF FROM TAP ON THIS BOARD (WHEN AND IF I CAN GET ON THIS BLOODY SYSTEM''). ALSO I MANAGED TO FIND A HUGE BOOK PUBLISHED BY AT&T ON DISTANCE DIALING (DATED 1975). DUNNO, IF ANYBODY'S INTERESTED THEN LEAVE A NOTE REQUESTING ANY INFO YOU'RE ARE CHEERS PS ANYBODY KNOW DEPRAVO THE RAT?? DOES HE STILL

LIVE?

Msg#: 7852 t*ACKER'S CLUB*
08/17/84 00:39:05 (Read 93 Times)
From: xxxxxxxxxx
To: ALL USERS
Subj: NKABBS
NKABBS IS NOW ONLINE. FOR ATARI & OTHER MICRO USERS. OPERATING ON 300 BAUD VIA RINGBACK SYSTEM. TIMES 2130HRS-2400HRS DAILY. TEL :0795 842324. SYSTEM UP THESE TIMES ONLY UNTIL RESPONSE GROWS. ALL USERS ARE WELCOME TO ON. EVENTUALLY WE WILL BE SERVING BBC,COMMODORE VIC 20/64 OWNERS.+NEWS ETC.

Msg#:8154 *EREWHON*
08/02/84 21:46:11 (Read 13 Times)
From: ANON
To: ALL
Subj: REPLY TO MSG# :1150 (PHREAK BOARDS)

PHREAK BOARD NUMBERS
ACROSS THE U.S.

IF YOU KNOW OF A BOARD THAT IS NOT LISTED HERE, PLEASE LET ME KNOW ABOUT IT.

JOLLY ROGER	713-468-0174
PIRATE'S CHEST	617-981-1349
PIRATE'S DATA CENTER	213-341-3962
PIRATE'S SPACE STATION	617-244-8244
PIRATE'S OUTHOUSE	301-299-3953
PIRATE'S HANDLE	314-434-6187
PIRATE'S DREAM	713-997-5067
PIRATE'S TRADE	213-932-8294
PIRATE'S TREK	914-634-1268
PIRATE'S TREK III	914-835-3627
PIRATE-80	305-225-8059
SANCTUARY	201-891-9567
SECRET SERVICE][	215-855-7913
SKELETON ISLAND	804-285-0041
BOCA HARBOR	305-392-5924
PIRATES OF PUGET SOUND	206-783-9798
THE INSANITARIUM	609-234-6106
HAUNTED MANSION	516-367-8172
WASTELANDS	513-761-8250
PIRATE'S HARBOR	617-720-3600
SKULL ISLAND	203-972-1685
THE TEMPLE	305-798-1615
SIR LANCELOT'S CASTLE	914-381-2124
PIRATE'8 CITY	703-780-0610
PIRATE-S GALLEY	213-796-6602
THE PAWN SHOPPE	213-859-2735
HISSION CONTROL	301-983-8293
BIG BLUE MONSTER	305-781-1683
THE I.C.'S SOCKET	213-541-5607
THE MAGIC REALM	212-767-9046
PIRATE'S BAY	415-775-2384

BEYOND BELIEF	213-377-6568
PIRATE's TROVE	703-644-1665
CHEYANNE MOUNTAIN	303-753 1554
ALAHO CITY	512-623-6123
CROWS NEST	617-862-7037
PIRATE'S PUB][	617-891-5793
PIRATE'S I/0	201-543-6139
SOUNDCHASER	804-788-0774
SPLIT INFINITY	408-867-4455
CAPTAIN'S LOG	612-377-7747
THE SILHARILLION	714-535-7527
TWILIGHT PHONE	313-775-1649
THE UNDERGROUND	707-996-2427
THE INTERFACE	213-477-4605
THE DOC BOARD	713-471-4131
SYSTEM SEVEN	415-232-7200
SHADOW WORLD	713-777-8608
OUTER LIMITS	213-784-0204
METRO	313-855-6321
MAGUS	703-471-0611
GHOST SHIP 111 - PENTAGON	312-627-5138
GHOST SHIP - TARDIS	312-528-1611
DATA THIEVES	312-392-2403
DANGER ISLAND	409-846-2900
CORRUPT COMPUTING	313-453-9183
THE ORACLE	305-475-9062
PIRATE'S PLANET	901-756-0026
CAESER S PALACE	305-253-9869
CRASHER BBS	415-461-8215
PIRATE'S BEACH	305-865-5432
PIRATE'S COVE	516-698-4008
PIRATE'S WAREHOUSE	415-924-8338
PIRATE'S PORT	512-345-3752
PIRATE'S NEWSTAND][	213-373-3318
PIRATE'S GOLDMINE	617-443-7428
PIRATE'S SHIP	312-445-3883
PIRATE'S MOUNTAIN	213-472-4287
PIRATE'S TREK][	914-967-2917
PIRATE'S TREK IV	714-932-1124
PORT OR THIEVES	305-798-1051
SECRET SERVICE	213-932-8294
SHERWOOD FOREST	212-896-6063
GALAXY ONE	215-224-0864
R.A.G.T.I.H.E.	217-429-6310
KINGDOM OF SEVEN	206-767-7777
THE STAR SYSTEM	516-698-7345
ALPHANET	203-227-2987
HACKER HEAVEN	516-796-6454
PHANTOM ACCESS	814-868-1884
THE CONNECTION	516-487-1774
THE TAVERN	516-623-9004
PIRATE'S HIDEAWAY	617-449-2808
PIRATE'S PILLAGE	317-743-5789
THE PARADISE ON-LINE	512-477-2672
MAD BOARD FROM MARS	213-470-5912
NERVOUS SYSTEM	305-554-9332
DEVO	305-652-9422

TORTURE CHAMBER	213-375-6137
HELL	914-835-4919
CRASHER BBS	415-461-8215
ALCATRAZ	301-881-0846
THE TRADING POST	504-291-4970
DEATH STAR	312-627-5138
THE CPU	313-547-7903
TRADER'S INN	618-856-3321
PIRATE'S PUB	617-894-7266
BLUEBEARDS GALLEY	213-842-0227
MIDDLE EARTH	213-334-4323
EXIDY 2000	713-442-7644
SHERWOOD FOREST][	914-352-6543
WARLOCK~S CASTLE	618-345-6638
TRON	312-675-1819
THE SAFEHOUSE	612-724-7066
THE GRAPE VINE	612-454-6209
THE ARK	701-343-6426
SPACE VOYAGE	713-530-5249
OXGATE	804-898-7493
MINES OF MORIA][	408-688-9629
MERLIN'S TOWER	914-381-2374
GREENTREE	919-282-4205
GHOST SHIP][- ARAGORNS	312-644-5165
GENERAL HOSPITAL	201-992-9893
DARK REALM	713-333-2309
COSMIC VOYAGE	713-530-5249
CAMELOT	312-357-8075
PIRATE'S GUILD	312-279-4399
HKGES	305-676-5312
MINES OF MORIA	713-871-8577
A.S.C.I.I.	301-984-3772

If Anybody is mad enough to actually dial up one (or more') of these BBs please log everything so thAt others may benefit from your efforts. IE- WE only have to register once, and we find out if this board suits our interest. Good luck and have fun! Cheers,

Msg#: 8163 *HACKER'S CLUB*
08/30/84 18:55:27 (Read 78 Times)
From: XXXXXXXXXX
To- ALL
Subj: XXXXXX
NBBS East is a relatively new bulletin board running from lOpm to 1230am on 0692 630610. There are now special facilities for BBC users with colour, graphics etc. If you call it then please try to leave some messages as more messages mean more callers, which in turn means more messages Thanks a lot, Jon

Msg#: 8601 *HACKER'S CLUB*
09/17/84 10:52:43 (Read 57 Times!
From: xxxxxxxxxx
To: xxxxxxxxx
Subj: REPLY TO Msg# 8563 (HONEYWELL)
The thing is I still (sort of I work for XXX so I don't think they

would be too pleased if I gave out numbers or anything else. and I would rather keep my job Surely you don't mean MFI furniture ??

Msg#: 8683 *HACKER'S CLUB*
09/19/84 19:54:05 (Read 63 Times)
From: xxxxxxxxx
To: ALL
Subj: DATA NODE
To those who have difficulty finding interesting numbers. try the UCL Data Node on 01-388 2333 (300 baud).When you get the Which Service? prompt. type PAD and a couple of CRs. Then, when the PAD> prompt appears type CALL XOOXOOX, where is any(number orrange of numbers. Indeed you can try several formats and numbers until you find something interesting. The Merlin Cern computer is 9002003 And it's difficult to trace You through aq data exchange! If anyone finds any interesting numbers, let me know on this board, or Pretsel mailbox 012495225.

Msg has replies, read now(Y/N)' Y

Msg#: 9457 *HACKER'S CLUB*
10/11/84 01:52:56 (Read 15 Times)
From: xxxxxxxxxxx
To: xxxxxxxxxxx
Subj: REPLY TO MSG# 8683 (DATA NODE)
IF YOU WANT TO KNOW MORE ABOUT THIS xxxxx PHONE PHONE xxxx xxxxxx ON 000 0000

Msg#: 8785 *HACKER'S CLUB*
09/21/B4 20-28-59 (Read 40 Times)
From xxxxxxxxxxxxx
Subj: NEW Number

NEW Computer ON LINE TRY RINGING 960 7868 SORRY THAT'S 01 (IN LONDON) IN FRONT. good LUCK!

Please note that none of these hints, rumours, phone numbers and passwords are likely to work by the time you are reading this... However, in the case of the US credit agency TRW, described in the previous chapter, valid phone numbers and passwords appear to have sat openly on a number of bulletin boards for up to a year before the agency realised it. Some university mainframes have hacker's boards hidden on them as well.

It is probably bad taste to mention it, but of course people try to hack bulletin boards as well. An early version of one of the most popular packages could be hacked simply by sending two semi-colons (;;) when asked for your name. The system allowed you to become the Sysop, even though you were sitting at a different computer; you could access the user file, complete with all passwords, validate or devalidate whomever you liked, destroy mail, write general notices, and create whole new areas...

Research Sources

The computer industry has found it necessary to spend vast sums on marketing its products and whilst some of that effort is devoted to 'image' and 'concept' type advertising--to making senior management comfortable with the idea of the XXX Corporation's hardware because it has 'hear