IAPetus

Quarterly Bulletin For the Institution of Analysts & Programmers

Issue 10 *July 1994*

Conference 1994

Friday, 21st October – this is the date to put in your diary.

The autumn Conference is the main event in the Institution's calendar. Once again we shall be returning to the City University, once again we have managed to hold the cost to £60 per head, which includes a 3-course lunch with wine.

As always, the papers will be presented mainly by our own members. There will be opportunities for questions and informal discussion, both with the presenters themselves and with members of the Council and Institution staff who will be present. Programming can be a solitary activity: here is an opportunity to air your ideas with fellow enthusiasts and perhaps learn something useful too. The papers to be presented not only reflect the interests of our members, but include topics of practical relevance to everyone in our industry.

So why should you attend the Conference? Because you will hear experts in their field cover topics like:-

Copyright Issues in Relation to Computer Software – In the light of recent cases this paper will deal with questions relating to the ownership and transmission of copyright in computer software and the ways in which such copyright may be infringed. It will also consider the issues resulting from the copying of interfaces and reverse-engineering.

Legal Issues in Software Contracts – Common clauses in software contracts will be discussed, and the presentation will seek to address the concerns of software suppliers in relation to the variety of clauses that purchasers of software will try to impose, including those relating to bespoke development work.

Information Systems Development – Why Structural Methods Fail – Structured methods are very popular for large development projects, but their usefulness is sometimes open to question. We will hear of the experiences in real project development and look at the reasons for failure. Alternative approaches will be discussed and potential problems and pitfalls explained.

The Teaching of IT to People in Prison – There is a view that the teaching of IT to people in prison is asking for trouble. However, in this paper we will learn how the teaching of IT, supported by companies and individuals, can enable people to obtain qualifications up to degree level and beyond. These qualifications can help prisoners to secure employment upon release and so break free of the vicious circle of crime.

EDI – Its Relevance and Implementation – Most of us have heard of EDI, but what benefits are there in it for us? How does it actually work? What investment is required? What are the problems? How can we make the technology work for us? These and other questions will be addressed.

One of the reply-paid cards sent with this copy of *IAPetus* can be returned to confirm your interest. Post the card now and we will make a provisional reservation for you and in due course send an invoice. Reservations will be confirmed when payment is received.

IAP Council Elections – *see page 7*

Inside this issue

Editorial

I suppose I'd better say something, so just before this little lot goes off to the printer...

A nice mixed bag for you. If you like cryptanalysis, have a need for secure data transmissions or just want to speculate about what the security services really do, Ted Pugh's latest on Vernam ciphers should keep you entertained. Just the thing to go with a large drink and a sunny spot to bask in.

How many of you take computers or computer magazines etc. on holiday with you? Or do your wives/boyfriends/pet canaries insist that you "switch off" entirely?

Alex and I went on a cruise this spring, he took a laptop... and spent every sea day thumping alien monsters! To the great amusement of the other passengers. Me, I indulged in "low tech word processing" – or in other words I wrote short stories with pen and paper.

Pay attention to the Conference date... and try to come along. Those who do enjoy the event, and it is good to be able to put faces to the names you read about in *IAPetus* and elsewhere. And I am the short fat one with long black hair going white!

Have a good summer,

Megan C. Robertson

The Director General Writes

I am writing these notes a week after the Council meeting, which had to be put back a few days because of the rail strike. As reported elsewhere a number of new Council members were elected on June 1st, and this was our first opportunity to hear their ideas.

One of the less weighty matters discussed was whether the Directory of Members should continue as a book, or whether it should be distributed on disk. There are three main considerations – cost, convenience for members and security of the information.

Now that we prepare the proofs ourselves, the main costs of producing the present Directory are printing and postage. We believe disks would be cheaper to produce and cheaper to mail. Furthermore as the membership grows disks would show an increasing advantage. The printed directories will get heavier and more expensive to post – disks would not!

In any event there seems to be a case for splitting the Register of Consultants away from the main Directory. Whereas most members understandably want to restrict access to their addresses, consultants for the most part we believe, would welcome wider publicity.

A Register of Consultants published separately, either as a book or on disk, and made available without restriction, could bring added benefits to consultants, and increased public awareness of the role of the IAP.

Because the details of consultants are held on disk (and constantly updated) at the IAP offices, we already have a limited search facility which can be mobilised in response to enquiries. Now we plan to develop a more sophisticated database, and the question has arisen as to whether this should then be made available on disk to members and outsiders so that they could carry out searches for themselves.

These considerations obviously concern all members, and we would be glad to hear from anyone who has strong views or fresh ideas on the subject. I can reassure you that the Institution's determination not to sell the addresses of the general membership or otherwise make life easier for the distributors of junk mail is undiminished.

I cannot finish without making a personal exhortation to all of you to make time to attend the 1994 IAP Conference. These are cheerfully informative occasions: already we have our "regulars" but we need some more. The details will be announced in the next edition of *IAPetus*.

Michael C. Ryan
Director General

The Job Search Process – A One Day Seminar

The Institution is pleased to announce a one day seminar designed to assist those of our members and ex-members who are involved in a job search either through the impending conclusion of a contract, redundancy or the threat of redundancy or, simply considering a career move.

With just a little awareness of what's required, the whole approach to job search changes. What should a modern day CV really look like? What do the recruiters really want? What image should the candidate present at interview? What are the key questions that keep coming up and how should we respond? How do we ensure a positive mental attitude? Where and how do we make others aware of our need and how should we build up a network of contacts who could help us into new employment?

Applying for a new job can be a losing game. There is only ever one winner. Hundreds lose. With the market for jobs as competitive as it is, getting a head start and staying in front of the competition becomes vital if success in job search is to be assured.

Those members who have experienced losing their job through redundancy will agree that it can be as traumatic as a bereavement or a divorce. Emotional stress runs high and depression usually follows. Most unemployed people need guidance to help them get back to work as fast as possible. With 70% of all jobs found through personal contact, contact development becomes a priority and CV preparation and interview presentation skills are paramount to success in job search.

All of these points and more will be addressed in the seminar. Depending on the interest registered we shall decide whether to hold a regional or London based seminar or both, probably in September. The leaders are Gordon Greenfield and Bob Collier who are already known to some of you through their previous assistance to members. So if you would like to know more please return the enclosed reply paid card.

Standing Orders

For a couple of years now the Institution has been encouraging members to pay their subscriptions by direct debit. Over half the membership is already benefiting from the savings provided by this method of payment.

However, a significant number of members now paying by direct debit have failed to cancel previous standing orders, so that small extra amounts of money continue to trickle into our old Natwest account at Twickenham.

Since the Institution was incorporated last year a new account has been opened with Coutts Bank in London. We want to close the Twickenham account but cannot do so while members keep paying money in.

Could we please urge all of you paying by direct debit to check that you have cancelled any previous standing orders. And would those of you still paying by standing order please think again about the savings you could be making by changing over to direct debits.

Just call Nicole at the Institution office and she will send you a form.

Dear Sir,

I was interested to read in *IAPetus* that the Institution is considering applying for a Royal Charter.

For some reason not clear to me, computer programmers tend to have a poor image and I feel that the letters C.Prog. would go some way towards improving things.

I agree that the Institution should not follow the BCS in seeking Chartered Engineer status. Part of my degree is in engineering but if people employ me this is not what they are paying for.

Programming is a profession in its own right and should be recognised as such.

I hope other members of the Institution will support the application for a Royal Charter as I believe it can do us nothing but good.

Yours faithfully,

Brian Darling BA MIAP

Student Experience

The plea in the last issue of *IAPetus* has so far yielded four students seeking experience and nobody prepared to offer it! Come on, you lot!

So far we have the following "eager beavers" who would like to widen their experience:-

Mark Bernard, in the third year of a Computer Science degree at Stirling University, who would like a placement in Central Scotland.

Herbie Daly, a student at Brunel University reading Computer Science. He speaks German and would welcome the chance to use his language skills, possibly overseas.

Bert Pachner, at Stafford University, known to you as "The Beginner", who also speaks German and has wide experience of stores management to offer.

Leslie White, who is studying maths and computing with the Open University and has been a home computer user since "the tender age of 10".

If your company has any openings for vacation work, or space for someone to get some work experience, please consider these people. More details of their skills are available from me, and I'll be glad to put you in touch with them.

A New IAP Branch...

Ronald Beaumont would like to hear from anybody in the Medway Towns area, or those prepared to go there, interested in getting together. He says:-

Branch topics – Security, Training, Visual Programming anything goes, less formal, beer...

Bi-monthly meeting (gathering is a better word), exchange of ideas, stories, mutual help, the usual sort of thing, but less heavy on work, more on social side, guest presenters.

In terms of venue, I have a large number of contacts who could provide anything we need.

If anyone is interested (you SHOULD be!) Ronald can be contacted by various means:

CIX	beaumor@cix.compulink.co.uk
Compuserve	100025.1106@compuserve.com
Telephone	0370 312266 (24 hours mobile)
	0634 220505 (19:30 – 21:30)
Snail Mail	10 Graveney Close, Cliffe Woods, Rochester, Kent ME3 8LB.
Fax	0634 220505 (24 hours)

Carrier pigeons welcome (may be eaten!)

"No apathy, no time wasters, no excuses!!!"

An Improved V

by Ted Pugh AFA FIAP

An interesting idea for an electronic cipher arose in 1917 when an MIT graduate by the name of Gilbert Vernam was working for AT&T.

His idea was to synchronise a teletype tape containing randomly produced 5 bit Baudot values with that of a message's plain-text.

Before transmission, each plain-text character was XOR'd with a corresponding character on the "key" tape while, at the receiving end, a duplicate key-tape was synchronised with the incoming message and the XORing process repeated.

Unfortunately, Vernam's cipher had two major weaknesses: the Baudot set contained only 32 different codes – with the result that the key stream soon began to repeat – and the same stream was reused to encrypt further messages. It was these features that rendered the method highly vulnerable to simple cryptanalysis.

Breaking the cipher

Take two Vernam transmissions and XOR these together. (The result is identical to having XOR'd the first plain-text with that of the second.) Now systematically select pairs of characters that produce the required value when XOR'd together and that also make sense in the context of both tentative texts.

The task is made easy with the help of a computer and made even simpler by cipher users beginning their messages in traditional style (like using "Dear Sir", including their address as a heading or regularly using the same signature block).

As both messages are deciphered, the key stream is subsequently revealed by XORing broken plain-text with its encrypted version. Nothing could be easier.

"the time taken to crack a 32 bit key-code is about 36 minutes. A 16 bit key takes around four seconds to break"

Key security

In an effort to improve security, modern Vernam implementations make use of 16 or 32 bit values to permit much longer key streams to be used. Many security professionals and the vast majority of manufacturers will point to this factor as indicating the cipher's security.

A 32 bit key, for example, supplies over four billion different seeds and, to the layman, may suggest odds of around four billion to one against a security breach. More realistically, one might expect a brute-force attack to require some 2 billion attempts to successfully locate a 32 bit stream's seed.

Now this may sound a lot, but with a sophisticated computer capable of carrying out one step per microsecond (one million steps every second) the time taken to crack a 32 bit key-code is about 36 minutes. A 16 bit key takes around four seconds to break.

More importantly, it can be shown that a 32 bit key may be unambiguously broken with a sample of just 40 plain-text characters. For a 16 bit key this is reduced to just 10. You don't need to be a mathematician to see how misleading odds-based calculations can be when discussing modern cipher security.

PRNGs

If the key stream used in the Vernam cipher was truly random we wouldn't need to worry too much about key size. If each value was as likely as any other then it follows that, without the proper key, every translation is as likely as any other too. In other words, a cryptanalyst may apparently succeed in recovering plain-text from an encrypted Vernam transmission, but it need not correspond to the original message.

If key streams were truly random, opponents could never be certain that their decryption was correct. However, key streams are not truly random. Instead, their production depends upon a suitable pseudo-random number generator (PRNG) algorithm – and any algorithm, given sufficient output data, can be reverse engineered.

PRNGs can be constructed in several ways (although the basic algorithm remains the same), a seed value is manipulated to produce a further number that then becomes the new seed when the process is repeated.

For speed and flexibility, a favourite method is to use congruent multiplication in conjunction with a prime modulus to generate the key stream. But like all PRNG methods it does have its weaknesses...

Algorithmic weaknesses

Consider the key stream: 8, 9, 6, 4, 10, 3, 2, 5, 7, 1... On the face of it, things look pretty random, but (using Y to indicate an unknown multiplier) we can extract $8Y = 9 \bmod P$ and $2Y = 5 \bmod P$ – simulating a cryptanalyst identifying the two stream sequences 8, 9 and 2, 5.

Now we can formulate: $8Y = 9 \bmod P$ and $8Y = 20 \bmod P$ which, by subtraction, reveals a prime modulus of 11. Then: $2Y = 5 \bmod 11$. So 2Y must equal 16 and Y must be 8. The algorithm is therefore: seed = seed * 8 mod 11.

Attentive readers will note that, using the above formula, the largest key must be equal to prime-minus-one and that this value, 10, is located in the middle of the stream when a seed of one is used.

Moreover, a seed of unity will always generate the algorithm's multiplier as the next stream value. Another interesting point is revealed when considering adjacent values with a displacement of six: 8 & 3, 9 & 2, 6 & 5, 4 & 7 and 10 & 1. Their sums all equal the value of the prime used, 11.

Some implementations try to make things more difficult by introducing a further modulo division to make the key stream appear "random with replacement". However, this only serves to complicate matters when a key is actually reduced by the additional division. For divisor-minus-one cases this will not be true and the standard attack outlined above will succeed.

Vernam Cipher

The word-size weakness

The main weakness overlooked by Vernam and his followers lies in the fixed size of the key values used. As we have already seen, knowing as few as two pairs of congruent keys can easily break some codes; although a little more analysis may sometimes be required.

At first sight, the following sequence appears insoluble: 9, 2, 7, 1, 9, 2, 6, 1, 6, 1, 7, 2, 0, 2, 9, 2, 5, 1, 3, 8, 2, 4, 1, 0. But when looked at as: 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24 and 10 it easily breaks open to reveal the algorithm: seed = seed * 3 mod 31.

The clue to a multi-digit key, in this example, arises from the frequency of digits and the presence of zero in the key stream. Normally we wouldn't expect to find zero unless congruent addition was being used, and we wouldn't expect to find so many instances of 1 and 2 compared with other digits.

Together, these observations point to a modulus of around 30 and discounts the possibility of the first two digits being read as 92. A similar logic applies to dismissing the incorporation of the value 8 into 38 or 82. It is far more likely to be a single digit number.

The suspected plain-text attack

One of the easiest ways in to someone else's transmission is through a suspected plain-text attack. Suppose our opponent believes that we invariably begin a message with the characters "Dear" – or that we invariably sign off with the string "Yours faithfully".

If true, it takes little effort to XOR expected text with an encrypted version to reveal part of the key stream – and much less to automatically analyses the exposed components to discover if they have a recognisable pattern.

Only two obstacles confront a cryptanalyst: determining the key size being used and obtaining a sufficiently large sample of the key stream to make analysis possible.

The latter requires sample plain-text greater or equal to twice the cipher's key length (since the idea is to reveal a pair of values for analysis) but, if the key size cannot be resolved, analysis is not possible (because there is no known ending point for a suspected key and therefore no way of determining its value). Herein lie sufficient clues to produce an unbreakable Vernam-type cipher without the need to generate streams of true random numbers.

A secure Vernam cipher

As indicated earlier, the presence of zero in the key stream can assist a cryptanalyst, but XORing plain-text with zero has no effect. There is therefore little point in making use of this key value.

By discarding all zero digits we ensure all plain-text is changed by the encryption process and disrupt an opponent's analysis. In addition, use of a variable length key disrupts analysis still further.

Consider the case of employing congruent multiplication with a suitable prime modulus of, say: 1, 067, 993, 517, 960, 455, 041, 197, 510, 853, 084, 776, 057, 301, 352, 261, 178, 326, 384, 973, 520, 803, 911, 109, 862, 890, 320, 275, 011, 481, 043, 468, 297.

Here, key lengths will vary between one and 97 digits in length and, just as importantly, the prime is large enough to ensure that a brute force attack is unlikely to succeed within any reasonable time span. (I calculate approximately 1.69×10^{82} years for the prime supplied here which, to give some perspective, is far greater than the estimated age of the universe – 1.5×10^{10} years.) Employing large, variable length numbers and discarding all zero components renders a plain-text attack futile.

With the above prime, the largest key generated would be: 1, 067, 993, 517, 960, 455, 041, 197, 510, 853, 084, 776, 057, 301, 352, 261, 178, 326, 384, 973, 520, 803, 911, 109, 862, 890, 320, 275, 011, 481, 043, 468, 296 which, if an opponent could recover it, would indicate the value of our prime.

But, by ignoring all zeros, the value prime-minus-one would only enter the key stream as the undersized: 16, 799, 351, 796, 455, 411, 975, 185, 384, 776, 573, 135, 226, 117, 832, 638, 497, 352, 839, 111, 986, 289, 322, 751, 148, 143, 468, 296.

Readers are cordially invited to suggest ways by which a cryptanalyst might identify this value, reinstate the zeros and thence derive our prime – preferably before our own sun turns supernova.

"Herein lie sufficient clues to produce an unbreakable Vernam-type cipher without the need to generate streams of true random numbers."

"Only two obstacles confront a cryptanalyst: determining the key size being used and obtaining a sufficiently large sample of the key stream to make analysis possible."

IAPetus is the Quarterly Bulletin of the **Institution of Analysts and Programmers.** The Editor is Megan C. Robertson. All views expressed herein are those of the authors, and do not necessarily reflect the Institution's or *IAPetus*' opinions or position. All material is © Copyright The Institution of Analysts and Programmers 1992. Produced by Breeze Ltd, 061-792 4442.
Correspondence about *IAPetus*, contributions etc. should be sent to the Editor at 12 Bude Close, Crewe, Cheshire CW1 3XG (Tel: 0270 500565). Correspondence about the Institution should be sent to Charles House, 36 Culmington Road, London W13 9NH (Tel: 081 567 2118, Fax: 081 567 4379).

The Beginner

I went to our local establishment of higher education today, hoping to find a place on one of these "Open Access" type courses, so that I could learn more about my friend (the PC). I spoke to a very efficient looking young lady behind a desk on which sat a beige box very similar to my own. She seemed to be having problems.

"Good morning" I said. "Bloody THING!" she replied. "I'm very sorry that you feel that way about me, perhaps I ought to speak to someone else."

"Oh, sorry, no not you, it's this, this, this ... BOX!"

"Why, what's the matter with it?"

"It's not working."

"May I have a look?"

A look of utter relief passed over the young lady's features. I walked around the desk to her side to be confronted by a blank screen, grey and lifeless. A quick check of the various connections showed that the power lead joining the VDU to the 'box' had become disconnected. Plugging it in brought flickers of life to the screen and happy noises from the young lady.

"How can I help you?" she asked. I explained my quest, explaining that as I was in receipt of Invalidity Benefit, following an attack of meningitis, I had quite a bit of time to spare.

"You'll want Mr. -*-*-*-*, I'll see if he's available. If you'll take a seat over there please."

I sat and waited. Groups of Oxfam fashion parade rejects ambled aimlessly to and fro, speaking in some form of code loosely based on the English language (I think). As I began to make a cigarette a loose bundle of animated woollens approached me. "You can't smoke here!" it said. O examined myself hurriedly but saw no signs of the offending vapours.

"No part of me appears to be burning at the moment" I replied, relieved. "But you're rolling a cigarette" the shape stated flatly. "Are you about to perform a strip-tease?" I asked, "Because you seem to be wearing clothes." Sounds of disgruntlement emerged from the layers of jumpers as it shambled off into the distance, to disappear through a set of double doors.

"Good morning".

I turned. A young man was standing to one side, a hand extended in greeting. "My name is David. I believe you have been waiting to see me." I rose. "Good morning, I'm Bert, I've come to enquire about learning more about my PC, however the receptionist says that you have no Open Learning facilities here."

We sat and talked for some time. David asked about my background and various questions about my machine. He then offered a guided tour of the computing facility that I eagerly accepted.

After the tour, during which I was questioned further, David took me to his office. "The local College will be running a computing foundation course, starting at the end of this year. If they accept you on that, I'll take you on as a student. Put yourself down for Computer Science initially and we'll sort it out when you get here, next year."

"??????????????????"

That afternoon, having telephoned from David's office to make an appointment, I presented myself to a Mrs. P.M.

We discussed my educational background (or lack of it) and my work history (I had taken a CV along, just in case) and I was asked to take a short Math/English test, 20 questions on an A4 sheet. Mrs. M, Pat, looked at my efforts and then surprised me by saying "Would you like to start this September?"

"??????????????????"

I am now a student, studying for a BSc (Hons) in Computer Science, linked to a modern language (I chose German), and some time in 1998 I will be drinking a bottle of champagne.

Win, lose or draw.

Bert is now well into his first year, enjoying his work and getting good grades too. Somehow I think that bottle of champagne will be a celebration.

❑❑❑

Already September is upon me. I arrived for "Induction Day", a sort of "Get to know your fellow students and have a quick look around" sort of day, in the week before the actual course started. We all wrote out cards with our first names on and placed them in front of ourselves on the desk. We were all given a big pile of forms to fill in and were asked to provide eight (?) passport-sized photos.

Mrs. M., Pat, was to be our course Tutor and gave us a short talk, which included the information that one student had already dropped out (does he know something that the rest of us don't?), then asked us, one at a time, to introduce ourselves and to say a few things about ourselves and our backgrounds.

No one seemed to wish to be the first, so after a bit I stood up. "Good morning, I'm Bert. I'm O L D" (The others all seemed to be aged about 14, except for one who was about my age.)

I gave a short potted history, about 8 minutes in all, then sat down and one of the other students did his bit. So it went on until we had all done more or less the same thing. We came from all sorts of backgrounds: Bus driver, Housewife, Market trader, Bouncer and so on. There were eighteen of us initially, already down to 17.

DER TAG

The alarm went off at 07:30 as planned. Get up, wash, shave, dress, walk the Dog (I hope he can get used to being alone all day), cup of coffee, cigarette, walk the dog, cup of coffee, check my bag... paper, pens, ruler, stapler, hole punch, pencils... cigarette... rubber (sorry, eraser), plain paper, squared paper... it's 08:00, cup of coffee, walk the dog, cigarette. NO I'M NOT NERVOUS ABOUT THIS, NOT AT ALL.

The first lesson was to be Business Organisation, at 09:30, followed by Quantitative Methods (Maths to you and me) then a Course Tutorial.

I left the Flat at quarter to nine for the 13 minute walk to the college. I went to the refectory (it's only a canteen really but I suppose I will have to learn to use these posh words now I'm here) for a coffee – 25p from a machine or 45p from the counter for coffee that's only marginally different although 4 flavours of difference are available.

You can't smoke inside, and there

Continued on Page 8

IAP Council Elections 1994

315 Voting cards were returned of which 2 were spoilt.

The following were elected to Council to serve for three years:-

Leslie Almeida
Gordon Bradley
David Daniel
Gavin Keeley
Ted Pugh

Thanks to the above and also to Stuart Shuttle who was the other candidate.

Voting Details

The voting was handled as a single transfereable vote for 5 individual places – this was to ensure that the representation was as fair as possible, and the voting was calculated as follows:-

Pass 1:	**Phase**	**1**	**2**	**3**	**4**	**5**	
	LA	91	93	96	111	144	
	GB	50	51	55	64		
	DD	18	19				
	GK	38	41	45			
	TP	105	108	113	129	156	< Elected
	SS	11					
	N/A	2	3	6	11	15	
Pass 2:	**Phase**	**1**	**2**	**3**	**4**		
	LA	119	122	129	161		< Elected
	GB	93	96	104	132		
	DD	26	31				
	GK	54	61	71			
	SS	20					
	N/A	3	5	11	22		
Pass 3:	**Phase**	**1**	**2**	**3**			
	GB	138	149	171			< Elected
	DD	49	54				
	GK	83	97	117			
	SS	33					
	N/A	12	15	27			
Pass 4:	**Phase**	**1**	**2**				
	DD	119	144				< Elected
	GK	114	140				
	SS	57					
	N/A	25	31				
Pass 5:	**Phase**	**1**					
	GK	182					< Elected
	SS	86					
	N/A	47					

The Great Virus Hunt

by T.N.W. Hynes SAM(R) HNC AMIAP

I recently had the dubious pleasure of curing a virus infection that had kindly been donated by the staff in our Egyptian office. The salesman arrived complete with his laptop, several diskettes and complaining bitterly that we had sent him a useless demonstration disk and "now my system doesn't work properly".

As I take great care to scan all our diskettes using 4 proprietary virus scanners and a couple of unique checksum generators of my own I was confident that I didn't send him a virus. However I immediately quarantined the laptop and disks and re-scanned all the master disks, image files and computers in my office.

Having ensured that all of these steps were in the green I then proceeded to investigate the suspect system. Not surprisingly I located the virus – CANSU – on the hard drive and one of the floppy disks. As is my usual procedure I made certain that I had a copy of the virus on disk and then began the clean up. This eventually led me to reformatting the hard disk as the partition table was totally garbage – in this case the loss was minimal as he had no major data stored on the disk.

The problem was cleared and I then set the network to re-running the scan routine (better safe than sorry!) whilst I sorted the relevant paperwork to inform the manager of the event.

At this point I had a vague recollection that I should report any virus occurrence to the police but I couldn't remember where or when I had read it.

Firstly I contacted the local police station. This caused some consternation as they were baffled as to how a person could catch a virus from a computer – "Surely this is a matter for Health & Safety?" Having calmed their fears of a possible epidemic of a new and bizarre disease I was able to get myself connected to the computer section. This turned out to be the purchasing section who didn't have any idea what to do or even if I had to report it.

Having met with little success I then called the IAP for advice. Whilst I didn't receive an instant answer I was given the numbers of 2 members who could help. Unfortunately I couldn't contact them immediately but as the infection was contained I could wait.

Having located the virus I then tested several other scanners and as I expected 2 of them failed to locate the virus. I have had this happen before due to a new strain or variant being imported from one of our satellite offices. I duly notified the software houses concerned and they were both very helpful. Neither company could enlighten me as to reporting but both requested a copy of the virus so they could investigate their scanner's failure.

I finally managed to contact David Eldridge who was able to give me a very interesting insight into the legalities and law surrounding a virus infection. Unfortunately he didn't know of any formal procedure but asked if I would let him know the result of my search. (Here it is!)

At long last I managed to contact Jim Bates who apart from being an expert on virus related problems is also a very busy man. Jim kindly took a short break to give me the details that I needed.

Yes, you do need to report a virus attack. You should report it to the Computer Crime Unit at New Scotland Yard. If you phone these people on 071 230 1177 they will send you a stack of extra information and the form you will need to complete and return in the event of an attack.

I would like to thank everyone who helped me in my search and leave everyone else with a few bits of advice that may help you in the future.

1. Don't rely on one package to be your guarantee against infection. A combination of scanners and techniques will give the best coverage.
2. Talk to or employ someone to help you set up a system of prevention. Any money spent in this manner will be repaid in security and peace of mind. But do make sure that the person you are dealing with is competent – the cost of an expert is not much more than your local "expert".
3. Don't trust to luck – it can and will happen. Prevention is better and cheaper than cure (if one is possible!).

The Beginner – *Continued from Page 7*

only seems to be enough seating for about 30% of those who are in there, the remainder either standing in bedraggled groups or sprawled around on the floor in various corners. Two eagle-eyed Security people amble about like somnolent Zombies watching equally "out to lunch" students. Part of our induction talk had been about College Security, this place appeared to be about as secure as water in a colander.

I went out for a cigarette and recognised a face, one of the students in my group. We chatted, strangers in a strange world. John, his name was, did a bit of gardening, felled a few trees, seemed totally out of place (he was the one who was about my age). I probably appeared equally out of place to him (it turned out that I am the eldest by about 5 years).

We made our way to the first class. The numbering system was strange. Room numbers beginning with "1" were not on the first floor but on the ground floor, those on the first floor began with "2", the letter prefix "E" did not mean East but paralleling E*** Street, one of the roads around the College. The "L" prefix was different again, it signified the block that linked "B" to "T". ????

My feet hurt, my legs ache, my head is swimming with "learning", something I haven't really done for a long, long time. I've walked Rusty (the Dog) and am sitting on my settee with my feet in a bowl of Radox'd hot water, coffee in one hand, cigarette in the other. Rusty has an immensely disapproving look on his face but I think he'll forgive me, I brought some dog-chocs back with me.

Me?... I think it's absolutely fabulous.

R.A. Pachner