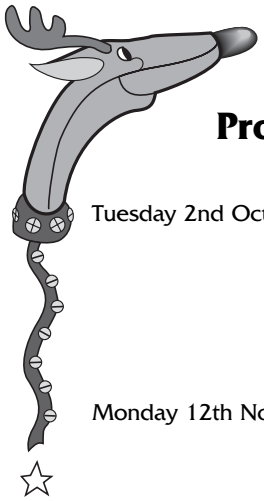
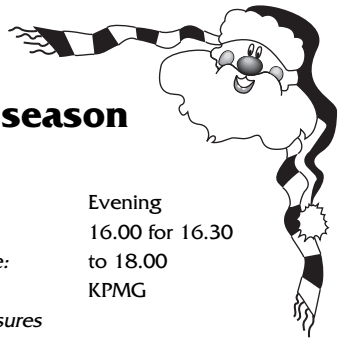
IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL
volume 12 number 2 winter 2001 ISSN 0961-9348





Programme for members' meetings 2001/2002 season

Tuesday 2nd October	**Windows 2000 Security** *Configuring NT securely is often a major hurdle - Windows 2000 adds many new challenges to a secure infrastructure. Risk minimisation strategies include: reviewing typical threats; using W2K security mechanisms pro-actively; customising administrative control; planning and implementing counter-measures securing Active Directory; the encrypting file system.*	Evening 16.00 for 16.30 to 18.00 KPMG
Monday 12th November	**Outsourcing & Out of Control Projects** *About 25% of software projects will be cancelled because they are late, over budget, have unacceptably low quality, or experience some combination of these problems. Outsourced operations have created new security threats and risks. Practical control measures are vital. The risks associated with outsourcing overseas and ecommerce operations will be considered.*	All Day 10.00 to 16.00 ICAEW
Tuesday 4th December	**Network Security & Management** *Changes in the technologies underlying computer networks are important to auditors because these have implications both for network security management and the audit of these arrangements. These implications provide today's theme concentrating by way of example on the audit of ATM (Asynchronous Transfer Mode) and Frame Relay.*	Evening 16.00 for 16.30 to 18.00 KPMG
Tuesday 29th January	**Internet Security** *The theme of the day will be internet security, but particularly Intrusion Detection systems. These are automated systems that monitor communications and operating systems, alerting operators of potential hacking attacks.*	All Day 10.00 to 16.00 Royal Aeronautical Society
Tuesday 12th February	**The Subversive Spreadsheet** *"A spreadsheet application can subvert all the controls in all other parts of an information system" (R. Butler, VAT Auditor, Customs & Excise). This talk by presenters from The European Spreadsheet Risks Interest Group shows the evidence. It discusses the risks, the audit and preventative methods*	Evening 16.00 for 16.30 to 18.00 KPMG
Tuesday 5th March	**The System's Down - Again!** *The unavailability of computer systems can give rise to serious problems for the continuing operation of the business. The ability to deal with or prepare for these problems is critical for business survival. The theme of the day is how business minimises their risk and will include high availability options, problem management and business continuity.*	All Day 10.00 to 16.00 Royal Aeronautical Society
Tuesday 14th May	**Data & The Law** *The legal risks and issues associated with IT and networking are not always well understood and often underestimated. This update on a fast changing area of the law is aimed at meeting the needs of risk management/audit professionals and providing opportunities for debate and discussion.* **This will be followed by the Annual General Meeting.**	Evening 16.00 for 16.30 to 18.00 KPMG

The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue maps see back page.

visit our website at www.bcs-irma.org

Contents of the Journal

Technical Briefings		Front Cover
Editorial	John Mitchell	3
Results from SETI Survey		4
From the Antipodes - ISO/IEC 17799	Bob Ashton	5
The Web Page - Seals of Approval	Andrew Hawker	6
SETI@home - A Massive Distributed Data Mining Exercise	Eric Korpela *et al*	7
BCS Matters!	Colin Thompson	11
Humour Page		13
The 231 Rules of Survival		14
Membership Application		21
Management Committee		23

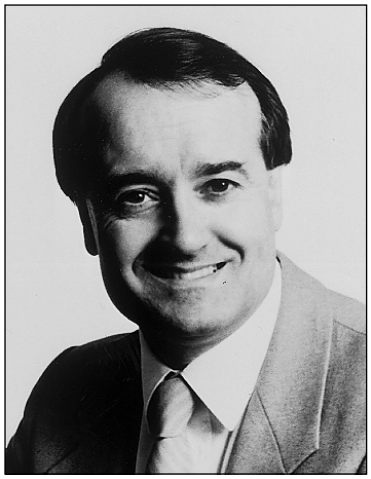
The ***Journal*** is the official publication of the Information Risk Management & Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL
Email: john@lhscontrol.com

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by PostScript, Tring, Herts.

Editorial



A little longer than usual, but with Christmas coming consider this my contribution to the season of good cheer.

First, a bumper humour section with another chance to win a prize while having fun. Second, Colin Thompson's BCS Matters column contains a wealth of information about the changes to our parent body, many of which will impact on this Group. Third, Andrew Hawker's web page deals with the thorny subject of trust and the Internet. Perhaps a contradiction in terms? Bob Ashton, our Australian correspondent finds more shortcomings in ISO17799, this time from the Australian government. However, the main article is not the usual academic dissertation, or even one of the more practical 'how to' expositions. No, it deals with the Search for Extra Terrestrial Intelligence (SETI) project that I have mentioned in previous columns.

Regular readers of the *Journal* will know of my interest in SETI. My interest is not so much that the ultimate outcome will be important for mankind, but rather the sheer scope of the data mining exercise and the use of distributed processing. There are also the underlying assumptions to be debated such as are we scanning the right energy spectrum? Both the scope of the project and the correctness, or otherwise of the underlying principles, are of particular interest to me as a computer auditor. Let us start with the principles. The assumption is that other intelligences will try to contact us by sending intelligible signals in the radio spectrum at frequencies that we can both detect and are listening to. This is a huge assumption. Even if it is correct, the secondary assumption, that the signals will be modulated in a way that we are familiar with and can decode is equally debatable. Let me provide an example. Most of our terrestrial radio signals currently transmit analogue information. In the near future that analogue transmission will be replaced by digital. This means that anyone listening on an analogue radio set will be unable to make sense of what they are receiving even though they are listening on the correct frequency. If off-world intelligences are broadcasting in some other medium then the entire SETI project is a waste of time. There are suggestions that pulsed light may be the communication medium of the future for us and for the others now. On the subject of which frequencies to listen to, the SETI assumption is that nature provides a nice way of establishing what these should be. The simplest 'stuff' of the universe, neutral hydrogen gas in interstellar space, emits radio signals at 1.42 GHz. Another molecule in space, the hydroxyl, or OH, emits at about 1.64 GHz. Now if you look at these two, H and OH, you would see that together they make up the compound of water HOH (or more commonly H_2O). Life as we know it requires water to evolve and exist. The frequency range between these two emissions, from 1.42 to 1.64 GHz, is therefore a region of the radio spectrum called the 'water hole'. Where would you expect water-based intelligent civilisations to meet? Around the water hole, of course! Good try for water based civilisations, but we are carbon based. So is the assumption correct? Only time will tell.

Applying this to my little world of audit I have noticed that most of my important findings have been as a result of detecting something that I did not expect. In many cases this was as a result of data mining rather than applying the laborious system

Continued on page 4

based audit approach. Hence my interest in SETI. As an example, I would not normally expect people of a male gender to have a hysterectomy, but I have found this interesting combination when data mining hospital patient records. The fact that I found it however, was because I could understand the underlying data structures. Unlike the SETI participants I could be sure of the communication medium. Having found the combination it was intuitive to examine the data quality rules on the assumption that the input validation routine was letting through an invalid combination. This was the case and my understanding of the data allowed me to detect a software anomaly. This is more difficult with SETI for two reasons. First we cannot be sure of the communication medium and secondly we do not know what the message should look like. A supporting example. I have also had my share of data mining failures based on an incorrect understanding of the communication medium. I once spent days trying to extract data from a file without success only to find that I was using an incorrect file layout description. My understanding of the signal was flawed. SETI could be in the same position.

How does my SETI data mining match up against the everyone else involved in the project? The table below provides the comparisons. You will notice that the time taken for me to complete a work unit is about five times the average. This is because my two machines operate at sub 300 megahertz speeds, which I suspect is a tad slower than those owned by the other participants. Despite my apparently low figures I have, according to the SETI statistics, completed more work units than 90% of the other participants.

As at 21 November 2001	Total	John Mitchell
Users	3,383,619	
Results received	399,604,453	214
Total CPU time	799,230.603 years	1.835 years
Floating Point Operations	1.142642e+21	Not available
Average CPU time per work unit	17hr 31min 13.7 sec	75hr 07min 50.7sec

If you are interested in data mining and would like to participate in SETI, then point your browser to http://setiathome.ssl.berkeley.edu. If you want to see a really good movie on the subject, then 'Contact' starring Jodie Foster, from a book of the same name by Carl Sagan, is the one to watch.

If you are aware of the concept of a 'delphic' poll you will know that if you ask a sufficiently aware and suitably large population it will intuitively predict the likely answer. On that basis the SETI survey (see below) predicts that we will detect the first ET signal within 100 years. Still too long for me, but if I see any little green men, or pink elephants for that matter, over the holiday period then they will probably be self inflicted! My computers however, will continue their patient search with unflagging attention. Assuming that the power stays on!

The compliments of the season and wishing you all the best for the New Year.

John Mitchell

P.S. Don't forget to check our web site **www.bcs-irma.org** for all the latest information.

Results from the SETI on-line survey as at 21 November 2001

Do you think there's life outside Earth? (102835 responses)

Yes	94.17%
No	1.47%
Not sure	4.36%

Should Earth send a signal for aliens to hear? (102605 responses)

Yes	78.23%
No	10.39%
Not sure	11.38%

Are aliens likely to be friendly or hostile towards us? (102535 responses)

Friendly	36.11%
Hostile	5.52%
Not sure	58.37%

What's your age range? (102618 responses)

0-12	0.29%
13-19	12.52%
20-39	61.51%
40-59	23.52%
60+	2.16%

What's your gender? (102401 responses)

Male	92.69%
Female	7.31%

How many computers do you have running SETI@home? (102628 responses)

1	58.63%
2-4	33.75%
5-9	5.59%
10-99	1.91%
100+	0.13%

Should the U.S. government fund SETI research? (102342 responses)

Yes	79.60%
No	11.56%
Not sure	8.84%

How many hours is your computer running on a typical day? (102505 responses)

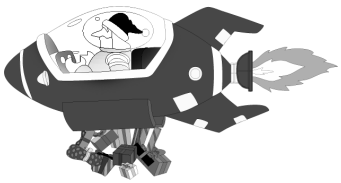
Less than 24	37.30%
24, because of SETI@home	34.19%
24, but not because of SETI@home	28.51%

What's your main reason for running SETI@home? (100328 responses)

Find ET for the good of humanity	58.34%
Find ET to become famous	3.03%
Keep my computer productive	16.35%
Get my name on a top 100 list on the web site	2.31%
Other	19.97%

When do you think humans will detect the first ET signal? (101377 responses)

Within the next 2 years	8.31%
Within the next 10 years	38.53%
Within the next 100 years	42.08%
More than 100 years from now	7.45%
Never	3.63%



From the Antipodes

Bob Ashton – Australian Correspondent

Australian Communication Security Instruction 33 (ASCI 33) and ISO 17799

ISO/IEC 17799, formerly BS 7799 and AS/NZS 4444, has been criticised in a number of fora. This standard had its origins in the early 1990's. At that time most commercial organisations had no connection to the Internet and e-commerce over the Internet was all in the future. This may well explain 17799's focus on controls over internal threats and its deficiencies in consideration of e-commerce and Internet sourced threats generally.

These shortcomings in 17799 have recently been addressed by the Australian Government's Australian Communications – Electronic Security Instructions 33 (ACSI 33) 2000 edition, produced by the Defence Signals Directorate (DSD), in Canberra. ACSI 33 is available from: **www.dsd.gov.au** and consists of 14 handbooks covering the following areas:

1. Standards
2. Evaluated Products
3. Risk management
4. Security Management
5. Emanations and Cabling Security
6. Media Security
7. System Access Control
8. Network Security
9. Cryptographic Systems
10. Web Security
11. Email Security
12. Malicious Software
13. Intrusion Detection
14. Physical Security

In Appendix D of Handbook 4 – Security Management, the DSD has highlighted ten 'key controls' from 17799 that are considered to be particularly important in IT security management. These ten control areas are recommended for use as a baseline for planning for security management activities or undertaking reviews of systems or sites. These key controls, including cross references to the relevant clauses in 17799, are listed below, together with a brief explanation of the intent of each of the controls.

1. Information Security Policy Document (Clause 1.1.2). This control is required to ensure the organization is clear on the security objectives relevant to the agency, and that endorsement for the policy has been granted by executive management.

2. Allocation of Information Security Responsibilities (Clause 2.1.4). Clear statements defining those staff or agencies responsible for security functions need to be agreed and promulgated.

3. Information Security Education and Training (Clause 4.2.2). One of the most important and effective security countermeasures is education and training of users and managers of the organization's information infrastructure.

4. Reporting of Security Incidents (Clause 4.3.2). It is critical that security incidents be addressed in a timely and thorough manner. Thought should be given to how best to deal with security incidents in the organization.

5 . Virus Controls (Clause 6.4.2). An increase in virus types and infection methods over the years has resulted in an overall increase in the threat likelihood of an information infrastructure being infected with a virus. An organization should therefore spend reasonable resources when addressing this problem.

6. Business Continuity Planning Process (Clause 9.1.2). The process to develop contingency plans needs to be dynamic and owned by the organization. There should be clear responsibilities and processes for developing these plans.

7. Control of Proprietary Software Copying (Clause 10.1.2). There are clear legal restrictions on the use of copyrighted material, and these restrictions should be formally observed and promulgated by an organization.

8. Safeguarding of Organizational Records (Clause 10.1.3). In all organizations, regardless of size, there are those records whose high levels of integrity, confidentiality and/or availability are critical to the operations of the organization. It is therefore important that these records be safeguarded.

9. Data Protection and Information Privacy Legislation (Clause 10.1.4). The organization must operate within the requirements of the law, including any relevant data protection and privacy legislation.

10. Compliance with Security Policy (Clause 10.2.2). Regular review of compliance with security policy should also be considered as necessary for effective security management.

Of particular value is the fact that throughout these Handbooks cross references for further guidance are made to other more detailed Australian Government information security related publications, some of which are freely available from DSD's web site or from the site of the Australian National Office for the Information Economy (NOIE). The availability of these guides means that DSD has effectively addressed the criticism that 17799 lacks detail.

As stated earlier, one of the most serious criticisms of 17799 is that it does not adequately address the risks associated with e-commerce. This is now well compensated for by the following ACSI 33 Handbooks:

- 8. Network Security
- 9. Cryptographic Systems
- 10. Web Security
- 11. Email Security
- 12. Malicious Software
- 13. Intrusion Detection

which provide a wealth of up to date material applicable to e-commerce security, and where appropriate are also cross referenced to the relevant clauses in 17799.

As an example, sound advice on Intrusion Detection can be found in Handbook13. Although this is an extremely topical subject, in my experience its implementation is still rare. Web Security might be even more important, and Handbook 10 contains a tutorial on how information recorded in standard web server logs can be used to compromise the privacy of persons doing no more than browsing the web server. This volume also contains a check list for web server security.

DSD has targeted the above advice on improving security in Government agencies. It is, however, equally applicable to the commercial sector.

The Web Page

Seals of Approval

Andrew Hawker

University of Birmingham

Christmas shopping on the Net is expected to reach record levels this year. But how can you tell whether a vendor is reputable? In some cases, the site will be operated by an instantly recognisable and reassuring high street "name". Even so, there is always the possibility that the brand or the URL has been hi-jacked by some unauthorised person, with devious plans for relieving you of your money. For smaller businesses with no strong brand name to rely on, customer confidence is particularly vital. Before committing to buy from these sites, people will want to be assured that their electronic transactions are secure, and that the goods or services will actually be forthcoming.

Many vendor sites now sport "Seals of Approval" which are aimed at improving customer confidence. Some of these concentrate on issues of security and privacy, such as **WebTrust** and **Truste**, while others promise fair dealing in all aspects of the transaction, for example in delivery, quality of goods, and the handling of complaints. Foremost among these in the UK is the **Which? Web Trader** scheme, which has around 2000 subscribers. In the US, similar schemes are run by **BBBOnline** (a subsidiary of the Council of Better Business Bureaus) and **ePublicEye**. (There appears to be rivalry between these two, with EpublicEye claiming to set "more demanding" standards for membership than BBBOnline).

For the consumer, the problem is that although all these schemes involve the use of impressive-looking symbols, there are wide variations in the extent to which they are backed up by any independent investigation or audit. WebTrust, for example, was originally launched by the leading accountancy bodies in the US and Canada, and involves a fairly rigorous appraisal of security measures in operation at each vendor's site. This makes it quite an expensive option, with strict conditions attached (such as a need for periodic review and re-certification). Only persons licensed by the accounting bodies can carry out the necessary audits. Perhaps not surprisingly, the list of clients for the US-based service is relatively short, although it includes some prestigious names. In other countries, including the UK, WebTrust has also been promoted by accounting professionals, with mixed success. Having launched its WebTrust service two years ago, the ICAEW is still actively marketing the concept, but makes no mention of a client list (see **www.icaew-webtrust.co.uk**).

Truste concentrates on privacy protection, and was set up in the US some five years ago as a non-profit organisation by various interest groups, including the Electronic Frontier Foundation. It claims a membership of 1500 sites, and operates around the world. However, its main base remains in the US, where privacy legislation has tended to be more fragmented and less strict than in Europe.

Another contender in the security stakes is **BT Ignite** service, which offers Trustwise certification in affiliation with Verisign. This service concentrates on vouching for the security of the web server, and the proper use of encryption: (it also perhaps suffers from an overdose of branding messages).

The more general commercial schemes, such as Which? Web Trader and BBBOnline, tend to be the easiest to join. Members sign up to a code of practice and give assurances about the way their site is being operated. They undertake to cooperate in resolving any complaints raised by customers under the scheme (and risk being thrown out if any complaints are upheld). In both these cases, the schemes are off-shoots of an organisation which is well established and well known, so that the parent body will have a vested interest in ensuring that everything is above board.

Other schemes are more a product of the Internet age. **ePublicEye**, for example, describes itself as a "trusted infomediary" in electronic commerce, and emphasises its track record in collecting customers' evaluations of the service from web sites. In the UK, another scheme to be found at **www.i-stores.co.uk** is also a child of the Net. It claims to offer its own "secure mark" and a "secure shopping directory", but little explanation is provided as to exactly what these terms mean, and it appears to function mainly as a trade directory.

Finally, some industry watch dogs have recognised the value of extending their remit on to the Net, and their emblems can be found on a number of sites belonging to the industry group in question. See for example the General Insurance Standards Council at **www.gisc.co.uk**, and the Federation of Small Businesses at **www.fsb.co.uk**.

Even the best-established schemes still have an experimental feeling to them. If symbols are "clickable" (as they should be) the results vary from scheme to scheme: some point you to a list of members, while others take you to a frame containing full background information and a dated certificate of membership. Some fail to work at all, which suggests that customers should be vigilant in checking that the symbols are indeed "active". However much of a rush you may be in over the Christmas shopping, it is probably worth taking the time to check whether the seal is genuine, and has not been pasted into the web page to try and impress you.

URL's of the sites mentioned above are:

WebTrust (USA) www.cpawebtrust.org

Truste (USA) www. truste.org

Which? Web Trader (UK) whichwebtrader.which.net

BBBOnline (USA) www.bbbonline.org

ePublicEye (USA) www.thepubliceye.com

BT Ignite/Trustwise (UK) www.ignite.com/uk/

A copy of this article, with embedded URL's will be posted to the IRMA web site three months after this edition has been circulated to members.

SETI@home

A Massive Distributed Data Mining Exercise

By Eric Korpela, Dan Werthimer, David Anderson, Jeff Cobb, and Matt Lebofsky

Since radio's earliest days, people have considered the possibility of detecting signals from an extraterrestrial civilization—and since the advent of radio astronomy, the tools to perform such a search have existed. Starting in the late 1950s, researchers have been performing progressively more sensitive searches, but each search has been limited by the technologies available at the time. As radio frequency technologies have become more efficient and computers have become faster, the searches have grown larger and more sensitive. The SETI@home project, managed by a group of researchers at the Space Sciences Laboratory of the University of California, Berkeley, is the first attempt to use large-scale distributed computing to perform a sensitive search for radio signals from extraterrestrial civilizations.

A radio SETI tutorial

You might wonder why an enormous supercomputer would be necessary to detect radio signals from an alien civilization. It might seem to be a fairly simple signal-processing task. Such a supercomputer is needed primarily because

- the parameters of an alien signal are unknown, and
- the sensitivity of a search for extraterrestrial intelligence (SETI) depends fairly heavily on the available processing power.

Our search for extraterrestrial intelligence assumes that an alien civilization wishing to make contact with other races would broadcast a signal that is easily detectable and easily distinguishable from natural sources of radio emission. One way to achieve these goals is to send a narrowband signal. By concentrating the signal power in a very narrow frequency band, the signal will stand out among the natural broadband sources of noise.

Consequently, radio SETI efforts have concentrated on detecting narrowband signals. When searching for narrowband signals, it is best to use a narrow search window (or channel) around a given frequency. The wider the channel, the more broadband noise is included in addition to any signal, which limits the system's sensitivity. Early systems used analogue technology to create narrow bandpass filters that could observe at a single frequency channel. More recent systems use massive banks of dedicated fast Fourier transform (FFT) processors to separate incoming signals into up to a billion channels, each 1 Hz wide.

Unfortuantely, this technique is limited. For one thing, extraterrestrial signals are unlikely to be stable in frequency because of transmitter and receiver accelerations. For example, a receiver listening for signals at 1.4 GHz located on the earth's surface undergoes acceleration of up to 3.4 cm/s^2 because of the Earth's rotation. That might not seem like much, but it corresponds to a Doppler drift rate of 0.16 Hz/s. If uncorrected, an alien transmission would drift out of a 1 Hz channel in about 6 seconds, effectively limiting the maximum integration time to 6 seconds. Because of the inverse relationship between maximum frequency resolution and integration time Du = (1/Dt), there is an effective limit to the frequency resolution that we can obtain without correcting the received signal for this effect (Du ~ 0.4 Hz).

In principle, we could correct for most of the drift resulting from the earth's motions, but how do we correct for an unknown planet's motions? An alien civilization narrowly beaming signals at the earth could correct the outgoing signal for the transmitter's motions, but a civilization transmitting an omnidirectional beacon could not make such an adjustment. Therefore, to search for this type of signal at very narrow bandwidth (<< 1 Hz) and the highest possible sensitivity, we would need to correct for Doppler drift at the receiving end and search for signals at multiple Doppler drift rates. Repeating an analysis at multiple Doppler drift rates becomes compute intensive.

Other signal parameters are still unknown—for example, at what frequency will it be transmitted? What is its bandwidth? Will it be pulsed? If so, at what period? Fully investigating a wide range of these parameters requires proportionally larger computing power.

In addition to detecting a signal, we must determine whether a signal is truly of celestial origin. The vast bulk of the narrowband signals received by a radio telescope consists of locally generated radio frequency interference (RFI). Fortunately, RFI has properties that let us distinguish it from extraterrestrial emission. But again, this RFI elimination requires computing resources.

Performing all of these calculations for even a small portion of the radio spectrum would require more computational power than is available in the largest existing supercomputer.

Distributing the load

Fortunately, searching for signals in a data stream from a radio telescope is an easily distributed task. We can break up data from an observation into frequency bands that are essentially independent of one another. In addition, an observation of one portion of the sky is essentially independent of an observation of another part. This lets us divide a large dataset into small chunks that a personal computer can analyse comparatively quickly. In this way, we can distribute the work to people willing to donate their spare CPU cycles.

SETI@home conducts its observations at the National Astronomy and Ionospheric Center's 305-meter radio telescope in Arecibo, Puerto Rico. The project uses a dedicated feed. This unique arrangement enables SETI@home observations without interference with other uses of the telescope and results in three

main modes of observation. If the primary feed is stationary, objects in the sky pass through the SETI@home instrument's field of view (0.1 degrees) at the rate of the earth's rotation (also known as the sidereal rate). An object would require about 24 seconds to transit the field. If the primary observer is tracking a source on the sky, the SETI@home receiver's beam slews across the sky at twice the sidereal rate. Occasionally, other observers could use the SETI@home feed to track objects on the sky.

During the project's course, SETI@home will view most portions of the sky visible with the Arecibo telescope three or more times. This includes stars with declinations (the celestial equivalent of latitude) between –2° and 38°, thoroughly covering about 25% of the sky.

The SETI@home system records a 2.5-MHz-wide band centered at the 1,420 MHz hydrogen line. Because this line would be of interest to astronomers of any species who were studying the galaxy, this frequency is one of the most likely locations for deliberate extraterrestrial transmissions. This 2.5-MHz band is recorded continuously onto 35-Gbyte DLT tapes using 2-bit complex samples. Each tape holds about 15.5 hours of data. The entire sky survey is expected to require 1,100 tapes, for a total of 39 Tbytes of data.

The recorded tapes are shipped to Berkeley, where we subdivide them into small work units on four splitter workstations. We divide the 2.5-MHz bandwidth data into 256 subbands by means of a 2,048-point FFT[1] followed by 256 eight-point inverse transforms. Because the 9,766-Hz-wide subbands are divided into lengths of 220 samples, each work unit corresponds to about 10 kHz of bandwidth and 107 seconds of duration. Subsequent work units overlap by 20 to 30 seconds to allow full analysis of signals that might be within a beam transit time of the end of a work unit. We transfer each work unit to temporary storage (capable of holding about 750,000 work units) for distribution to users.

The main SETI@home server consists of three Sun Enterprise 450 series computers. One holds the user database, containing information on each of the 3.4 million SETI@home volunteers (including the number of work units completed, time of last connection, and team membership). The user database also holds information on the amount of work done by each type of microprocessor architecture and by each operating system to which SETI@home has been ported.

The second server system holds the science database in an ever-expanding array of redundant disks (currently a 432-Gbyte RAID 0+1). The science database contains information on the time, sky coordinates, frequencies, and so forth for each work unit generated, as well as information about how many times the work unit has gone to SETI@home users and how many results have been received.

The largest portion of the science database capacity stores the parameters of potential signals (such as signal power, frequency, and arrival time sky coordinates) detected by SETI@home volunteers. As of October 2000, the database contained 1.1 billion candidate signals (before RFI rejection).

The third server system contains the work unit storage, handling distribution of work units and storage of returned results. Communications between the server and clients use the hypertext transfer protocol (HTTP). We chose this protocol because many Internet volunteers might be behind firewalls that prohibit most traffic but permit access to the World Wide Web.

[1] Fast Fourier Transforms

The server supports two types of request. The first requests a work unit. The response to this request includes a work unit chosen from temporary storage. Priority goes to those units that have not previously been sent or those that were sent but for which no results were received.

In the second type of request, the client program returns a result to the server. The server inserts the candidate signals contained in the result into the science database and updates the volunteer's statistics in the user database. The response to this request includes the volunteer's statistics so that the client program can display them.

The SETI@home client program

SETI@home currently distributes client software for 47 different combinations of CPU and operating system. Users can download the software from the SETI@home Web site (**http://setiathome.ssl.berkeley.edu**). For Microsoft Windows and Apple Macintosh, the software installs itself by default as a screen saver, only processing data when the screen saver is active. For other platforms, the basic client is text based. Users of these platforms generally run the client in the background. A graphical display program similar to the Mac and Windows versions is available for Unix systems that run the X Windows system. In addition, a wide variety of third-party applications have been developed for display of data, detected signals, sky maps, and volunteer statistics.

After receiving a work unit, the client performs a baseline smoothing on the data to remove any wideband (Du > 2 kHz) features. This prevents the client from confusing fluctuations in broadband noise (due in part to variations in the hydrogen line emission as the field of view transits the sky) with intelligent signals. The client then begins the main data analysis loop, shown schematically below.

```
for Doppler drift rates from -50 Hz/s to +50 Hz {
for bandwidths from 0.075 to 1220 Hz in 2X steps {
Generate time ordered power spectra.
Search for short duration signals above a
constant threshold (spikes) for each frequency {
Search for faint signals matching beam
parameters (Gaussians)
Search for groups of three evenly spaced
signals (triplets)
Search for faint repeating pulses (pulses)
}
}
}
```

At the start of each passage through the loop, the data is transformed into an accelerated frame of a given Doppler drift rate. The drift rates at which the client searches the data for signals vary from –10 Hz/sec to +10 Hz/sec (accelerations expected on a rapidly rotating planet) in steps of 0.0018 Hz/sec. The client also examines the data at Doppler drift rates out to ±50 Hz/sec (accelerations of the magnitude that would arise from a satellite in low orbit about an earth-like planet), but at a more coarse step of 0.029 Hz/sec. A signal from an alien world would most likely have a negative drift rate (as the accelerations involved would be away from the observer). Despite this, we examine both positive and negative drift rates for the purpose of statistical comparison and to leave open the possibility of detecting a deliberately chirped extraterrestrial signal.

At each drift rate, the client searches for signals at one or more bandwidths between 0.075 and 1,221 Hz. This is accomplished by using FFTs of length 2^n (n = 3, 4, ..., 17) to transform the data into a number of time-ordered power spectra. To avoid repeating work, not all bandwidths are examined at every Doppler drift rate. Only when the change in drift rate becomes significant compared to ($1/Du^2$) does the program compute another FFT of a given length. Therefore, 32k-point transforms are performed one quarter as often as 64k-point transforms.

The transformed data is examined for signals that exceed 22 times the mean noise power. This threshold corresponds to 7.2×10^{25} W/m^2 at our finest frequency resolutions, or the equivalent of detecting a cell phone on one of the moons of Saturn. The SETI@home client reports any such spike signals in the resulting transmission.

If there is sufficient time resolution in the transformed data ($n < 15$) and the SETI receiver is not tracking an object on the sky, the client examines it for signals that match the telescope beam's parameters. As a radio source drifts through the field of view, the measured power will vary depending on the telescope's beam profile, which is approximately Gaussian. The SETI@home client performs a weighted c^2 fit on any signals that exceed 3.2 times the mean noise power and reports those for which the goodness of fit exceeds a certain level. This power level typically corresponds to 8.4×10^{-25} W/m^2.

The client then divides transformed data at each frequency into chunks with duration equal to the time required for an object to transit the telescope field of view. Two algorithms serve to analyze these chunks for pulsed signals. The first algorithm, the triplet finder, searches each chunk for three evenly spaced signals that each exceed 7.75 times the mean noise power (as little as 5.3×10^{-25} W/m^2) and report any detected signals.

The second algorithm is a modified fast-folding algorithm. A folding algorithm divides the data into chunks of duration equal to the period being searched and co-adds them to improve signal-to-noise ratio. An FFA performs this function on a large number of periods without duplicating additions. The SETI@home folding algorithm searches roughly $N \log N$ pulse periods, where N is the length of the input array. This corresponds to periods between two samples and $N/3$ samples. During a typical run of the client, this typically means half a million periods between 2 ms and 10 s. The program computes the threshold for detecting a pulsed signal dynamically to match the number of co-added samples. This threshold can be as low as 0.04 times the mean noise power for pulses with periods less than 10 ms. This corresponds to pulse energies of about 1.8×10^{-26} J/m^2.

Depending on the individual work unit's parameters, this processing loop requires 2.4 to 3.8 trillion floating-point operations (Tflop). It takes a typical (500 MHz) home computer 10 to 12 hours to complete a work unit. For an average work unit, the SETI@home client would report eight signals – four spike signals, one Gaussian, one pulsed signal, and one triplet signal.

Postprocessing

When the client has done its work, the job isn't done. Typically, the SETI@home client programme returns a few potential signals per work unit. Of course, not all of these signals are evidence of extraterrestrial intelligence.

Errors made in the processing computers cause some of the signals. Typical numeric processors, memory, and disk systems are fairly reliable. However, SETI@home uses thousands of years of CPU time per day, magnifying even low error rates. Even if undetected errors occur only on average every 10^{18} machine instructions, SETI@home would see several per day. Additional errors can be introduced in result transmission because of broken connections or malfunctioning HTTP proxies. To combat these effects, we examine each signal to see if the parameters match their permitted values. We also send each work unit to multiple volunteers and cross-check the returned values to verify accuracy.

The vast majority of the database's signals are evidence only of terrestrial intelligence. Sources of narrowband radio emission are ubiquitous where human technology is present. Even at the Arecibo observatory, where care is taken to minimize interference, this noise is present, due to local equipment, aircraft, satellites, and other transmitters. Fortunately, these terrestrial emissions are fairly easy to distinguish from an extraterrestrial signal.

A large fraction of RFI consists of continuous narrowband signals generated at or near the observatory. An extraterrestrial signal will only be detected when it is within the telescope's field of view, and, for our scanning mode of operation, will only have limited duration. Any signal that exceeds this duration must be terrestrial and may be rejected.

Other RFI sources are of short duration and repeat on time scales of hours to days. Therefore, any signal that repeats when the telescope is viewing a different portion of the sky might also be rejected.

After RFI is removed, the bulk of the remaining signals are due to random fluctuations in the noise background mimicking an extraterrestrial signal. To sort out the true extraterrestrials, we can look for persistent signals. We expect that an extraterrestrial signal will be present at a similar frequency the next time we examine the same celestial location.

A status report

As of 21 November 2001, 3,383,619 volunteers had run the SETI@home program. Of those, 519,725 were actively running the program and had returned a result in the previous two weeks. These volunteers had donated a total of 799,230 years of CPU times. Currently, the average processing rate of computers running SETI@home is 15.7 Tflops—averaged since the start of the project, the processing rate is 9.5 Tflops. To our knowledge, SETI@home is the largest distributed computation project in existence. It could also be considered to be the largest supercomputer in existence and the largest computation ever performed. While we were writing this paragraph, 60 new volunteers joined the project.

The 2.1 billion signals in the SETI@home database are being examined with the techniques we've described. The rate at which we are currently examining signals is lower than the rate at which new signals are being added to the database, so we have looked in detail at only a fairly small fraction of the potential signals. We will soon add another computer system to our server setup to speed this processing along – we hope to examine signals in real time before too long. So far, none of the signals examined has shown evidence of extraterrestrial intelligence.

Conclusion

SETI@home was originally slated to process two years worth of data from the Arecibo telescope. The strong public response and new improvements to the client software have prompted us to extend the survey.

SETI@home currently samples only a small portion of the radio spectrum and a small portion of the sky. The two most obvious means of expanding its capabilities are to expand the sky coverage and widen the frequency bandwidth. SETI@home II, currently under study, hopes to do both.

The best means of expanding the sky coverage would be to add a SETI@home recorder system to a southern hemisphere radio telescope. This would let us increase our sky coverage from about 25% to 75%. We are currently discussing the possibility with a southern observatory.

The recording system currently limits our frequency bandwidth. By duplicating the recording system, we could double SETI@home's bandwidth coverage (and, of course, its data rate).

As in any voluntary organisation, it's important that SETI@home be responsive to the desires of its volunteers, because the programme's success depends entirely on the volunteers who provide the computing resources. We will continue to keep our volunteers informed of our progress and to share with them the science behind SETI. We will also work to show our volunteers how they have individually contributed to the project by providing information about potential signals they have detected and the areas of the sky they have scanned.

Acknowledgments

SETI@home is largely funded through private donations. The SETI@home team especially thanks the Planetary Society, Sun Microsystems, Fujifilm, the SETI Institute, and Friends of SETI@home (private individuals) for their contributions. Some corporate contributions have been matched through the University of California Digital Media Innovation Program. We would also like to thank SETI@home volunteers everywhere for their valuable contribution of the processing power that makes SETI@home work.

References

S. Bowyer *et al.*, "Twenty Years of SERENDIP, the Berkeley SETI Effort: Past Results and Future Plans," *Astronomical and Biochemical Origins and the Search for Life in the Universe*, C.B. Cosmovici, S. Bowyer, and D. Werthimer, eds., IAU Colloquium No. 161 (Editrice Compositori: Bologna), p. 667, 1996.

D. Anderson *et al.*, "Internet Computing for SETI," *Bioastronomy 99: A New Era in Bioastronomy*, G. Lemarchand and K. Meech, eds., ASP Conference Series No. 213 (Astronomical Society of the Pacific: San Francisco), p. 511, 2000.

Eric Korpela is a research astronomer at the Space Sciences Laboratory at the University of California, Berkeley. In addition to his SETI work, he specializes in the study of interstellar matter and far ultraviolet astronomical instrumentation. Contact him at korpela@albert.ssl.berkeley.edu.

Dan Werthimer is director of the Serendip SETI program and chief scientist of SETI@home. He has published numerous scientific papers in the fields of SETI, radio astronomy, instrumentation and science education, and is editor of Astronomical and Biochemical Origins and the Search for Life in the Universe.

David Anderson is the SETI@home project director. David has done extensive research in operating systems, distributed computing, and computer grahics. David has recently joined the management team of the distributed computing provider United Devices as chief technology officer.

Jeff Cobb is a software engineer and systems manager for the UC SETI projects. He has been with the SETI group for seven years, and has developed many of the algorithms used in SETI@home.

Matt Lebofsky studied computer science and music composition at Binghamton University, and currently has two completely separate careers in both fields. (See also www.lebofsky.com.)

We are grateful to the authors and the Institution of Electrical Engineers (IEE) for permission to reproduce this article.

BCS MATTERS!

Colin Thompson
BCS Deputy Chief Executive

Colin Thompson, BCS Deputy Chief Executive, reviews some of the current BCS news items. Further information on these or any other BCS related issues may be found on the BCS Web site ("http://www.bcs.org.uk/")

Information is also available from Customer Services at The British Computer Society, 1 Sanford St, Swindon SN1 1HJ (e-mail to marketing@hq.bcs.org.uk)

The new BCS organisation arrives

After several years of planning, starting with the Pollard Review in 1998, the new BCS organisation was finally launched at the AGM on 25 October. Council remains unchanged as do the two main Executive Committees of Council, the Policy and Resources and Financial Operations Committee but, below that, we now have a new structure comprising 4 Boards and 3 Forums:

Member Services Board

Vice-President Charles Hughes; responsible for ensuring that the Society is providing its members and other interested parties the information and related services necessary for effective professional practice at all levels.

Knowledge Services Board

Vice-President Professor Wendy Hall; responsible for developing and disseminating a wide variety of knowledge about IS and its application to the IS professional community, business management and educational establishments.

Qualifications and Standards Board

Vice-President John Chapman; responsible for all aspects of the definition and accreditation of standards, including those relating to the admission to BCS professional membership. The responsibility also includes BCS examinations and the accreditation of academic courses and employer training schemes.

External Relations

Vice-President David Morris: responsible for establishing the Society as the recognised authoritative source of leadership in IS practice

Engineering and Technology Forum

Vice-President Professor John McDermid; responsible for providing a grass roots network of engaged practitioners, which will encourage the exchange of ideas and common interest, influence the work of the Society and support its programmes.

Education and Training Forum

Vice-president Lesley Beddie; responsibilities are similar to those of the Engineering and Technology Forum, but in relation to the IS education community, including the teachers.

Management Forum

Vice-President Rachel Burnett; responsibilities are as for the other Forums, but in relation to the IS management community.

As regular readers of this column will be aware, this reorganisation is part of a much wider modernisation of the Society, that includes the new branding and Web developments, and which requires a significant shift in the culture of the BCS. But new organisational structures cannot, of themselves, change the culture and it is for that reason that October 25th represents not just a new set of organisational labels but a very significant shift in the way that we do things. So, the new Boards and Forum Management Committees will be smaller than their predecessors – a maximum of 16 people – and will be much more focused on action and activity than on debate. The system of cross representation, which effectively ensured that each Board and Committee had representatives from a multitude of others, has now disappeared and the sole criterion for selection for Board or Committee membership will be the contribution that the individual can make to the work of that Board or Committee.

The focus on activity will be achieved through an enhanced planning process, under which each of the Boards and Committees will make an annual report the Policy and Resources Committee, setting out proposed objectives for the coming year and identifying achievements against the previous year's objectives.

Part of the aim, in implementing the new organisation, was to attract 'new blood' into the Boards and Committees and the success on this front was evident from the attendance at a BCS 'Top Team Conference' in London on 31 October. The one-day conference included the first meetings of the individual Boards and Forum management Committees and it was clear that the attendees included a significant number of new faces.

The Member Services Board

The member Services Board, under the leadership of Charles Hughes, is at the forefront of the push to make the BCS more member and customer focused. Charles himself is absolutely clear about the priorities for the new Board; they are, he says,

> *'to measure and monitor member attitudes and aspirations, ensure information and services are directed to meet member needs, and identify and lead the planning of new services and ensure these are delivered'.*

As part of its remit, the Board takes over the responsibilities of the old Branches Board for the Branches community and those of the old Technical Board for the Specialist Group community. Day to day management of the Specialist group community will be handled by a Management Committee, elected by the community, and representation at Board level will be guaranteed by the provision, that the Chair and Vice-Chair of that committee will be Board members by right. Elections will be part of the business of a regular 'Specialist group Assembly' that must be held at least once each year but, in practice will probably be held at 6-monthly intervals. The current representatives are Brian Layzell, as Chairman of the SG management Committee and Howard Gerlis, as Vice-Chair. Very similar arrangements are in place for the Branches Community.

The next meeting of the Specialist Group Assembly is due to be held in Spring 2002.

Member Survey 2001

Measuring our performance on the basis of member and customer perception, rather than by a supplier view of the world, will be an important feature of the new BCS. It is the

intention that information gained last year as part of an extensive member survey should be updated annually and the first of these update survey forms is now on the BCS Web site at http://www.bcs.org/survey2001/ .

If you are a member of the BCS do please complete the form; your input really is required if we are to provide the service that our members need.

Specialist Group Support

One of the objectives for the new organisation is to capitalise more effectively on the added value that the Specialist Groups provide. Someone once described the Groups as the 'hidden gems of the BCS' and the aim now is to provide a level of support which will ensure that the group activities gain greater visibility and that they are able to maximise the value of the contribution that they make, both to their own members and to the objectives of the Society as a whole.

Part of the required support will come from the new Web-based facilities, of which more later, but it will also require additional staff support within BCS headquarters. To cover the latter we now have approval for the new post of 'Specialist Group Support manager' and the first incumbent of that post, Nick Web, will be joining the staff in early December. A major part of his role will be to establish effective working relationships with the officers of each of the groups and to ensure that we can assist both in resolving problems and in exploiting opportunities as they arise.

The Web Initiative

The BCS Web Enablement Project is moving forward a little less swiftly than we had hoped – perhaps inevitably, given the complexity involved in linking the back-office systems, including the membership database, to the web. However, we expect the first tranche of the new facilities to be on stream early in the new year and additional functionality will then follow fairly rapidly. One of the first features will be the ability for each member to access and amend his or her details on line.

These developments will also provide important new support facilities for the Specialist Groups, including the ability to hold the details of Group members on the main BCS membership database and to update the details of those members on-line. Group members who are held on the membership database on this basis will be able to access and amend their own details. Alongside these facilities, Groups will have access to modern list-server facilities, linked to the membership database so that they will be able to e-mail their members on the basis of a list that is automatically updated to reflect the latest address information.

The new Web-based facilities will provide other opportunities to improve support services, and a small, representative group is being formed to advise HQ staff on requirements. The results of that work will be circulated to all Specialist Groups for comment in due course.

Information Systems Quality at Work

Not all our attention is given over to the reorganisation of course, and the Development Department has been busy designing and implementing a new employer accreditation scheme under the label ISQW.

The ISQW Award, builds on the experience of the BCS Professional Develoment Scheme since the late 1980's and part of the aim is to update those arrangements to reflect the current needs of practitioners and their employers. The award recognises the vital role training and development has in maintaining and updating employees skills sets and it is designed to encourage, support and recognise best practice within employers' career development processes and procedures. Based around a clear set of critical success factors and key performance indicators, it is awarded only to those organisations who have achieved formal accreditation, either on the basis of the organisation's own career development scheme or through the use of an 'off the shelf' solution provided by BCS.

BCS IT Awards

It is IT Awards time again and this year's winners were unveiled at a gala dinner at Le Meridien, Piccadilly held on 7 November. Sixty-three projects were submitted this year and the judges selected the eventual winners from a short-list of seven. Two overall winners, Exodus and The Virtual Railway, were selected and the awards were presented by Guest of Honour, Dame Stephanie Shirley.

The Exodus suite of software is a computer based laboratory for evaluating emergency and non-emergency movement and behaviour of people in aircraft, buildings and ships. Exodus simulates people-people, people-fire and people-structure interactions. It tracks the path of each individual as they make their way out of the enclosure, or are overcome by fire hazards such as heat, smoke and toxic gases. It provides a cost effective way to achieving safer and more functional designs, allowing designers and regulators to seek answers to questions that cannot be addressed using conventional approaches.

The Virtual Railway, is part of the Thameslink 2000 Project, a key strategic transport initiative designed to enhance and expand the existing Thameslink network throughout London, the Southeast and East of England. The Virtual Railway project from Bechtel, Railtrack and Infrasoft Solutions Ltd integrates the data and engineering disciplines required for this work, enabling experts working on stations, track, overhead power lines, substations, civil engineering and signalling, to all work from a common database, with the impact of any proposed changes quickly available to all concerned. The latest 3D Database Modelling and Visualisation technology allows a virtual railway to be designed and analysed prior to any building work, thereby improving design integration, standards of safety and construction. The team is now planning a 3D simulation of the entire Thameslink 2000 route.

And Finally.....

News of another change at the top of the Society. Judith Scott, the BCS Chief Executive since 1995, has announced her decision to retire in 2002. Judith's period in office has been one of very considerable success for the Society and she will be a hard act to follow. But, as readers of *The Times* newspaper will know, the search is now on for a successor.

HUMOUR PAGE

Dear Teechar!

These are actual excuse notes from parents (including original spelling) Collected by Nisheeth Parekh, University of Texas Medical Branch - Ed.

My son is under a doctor's care and should not take P.E. today. Please execute him.

Please excuse Lisa for being absent. She was sick and I had her shot.

Dear School: Please ekscuse John being absent on Jan. 28, 29, 30, 31, 32, and also 33.

Please excuse Gloria from Jim today. She is administrating.

Please excuse Roland from P.E. for a few days. Yesterday he fell out of a tree and misplaced his hip.

John has been absent because he had two teeth taken out of his face.

Carlos was absent yesterday because he was playing football. He was hurt in the growing part.

Megan could not come to school today because she has been bothered by very close veins.

Chris will not be in school cus he has an acre in his side.

Please excuse Ray Friday from school. He has very loose vowels.

Please excuse Pedro from being absent yesterday. He had (diahre) (dyrea) (direathe) the shits. [words in ( )'s were crossed out].

Please excuse Tommy for being absent yesterday. He had diarrhea and his boots leak.

Irving was absent yesterday because he missed his bust.

Please excuse Jimmy for being. It was his father's fault.

I kept Billie home because she had to go Christmas shopping because I don't know what size she wear.

Please excuse Jennifer for missing school yesterday. We forgot to get the Sunday paper off the porch, and when we found it Monday, we thought it was Sunday.

Sally won't be in school a week from Friday. We have to attend her funeral.

My daughter was absent yesterday because she was tired. She spent a weekend with the Marines.

Please excuse Jason for being absent yesterday. He had a cold and could not breed well.

Please excuse Mary for being absent yesterday. She was in bed with gramps.

Gloria was absent yesterday as she was having a gang over.

A FEW WORDS FROM THE VISIONARY STEVEN WRIGHT

A clear conscience is usually the sign of a bad memory.

If you must choose between two evils, pick the one you've never tried before.

A fool and his money are soon partying.

Plan to be spontaneous tomorrow.

If you think nobody cares about you, try missing a couple of payments.

Drugs may lead to nowhere, but at least it's the scenic route.

I'd kill for a Nobel Peace Prize.

Borrow money from pessimists - they don't expect it back.

Half the people you know are below average.

99 percent of lawyers give the rest a bad name.

42.7 percent of all statistics are made up on the spot.

A conscience is what hurts when all your other parts feel so good.

If you want the rainbow, you must put up with the rain.

All those who believe in psychokinesis raise my hand.

The early bird gets the worm, but the second mouse gets the cheese.

I almost had a psychic girlfriend but she left me before we met.

OK, so what's the speed of dark?

How do you tell when you're out of invisible ink?

If everything seems to be going well, you have obviously overlooked something.

Depression is merely anger without enthusiasm.

When everything is coming your way, you're in the wrong lane.

Ambition is a poor excuse for not having enough sense to be lazy.

Hard work pays off in the future. Laziness pays off now.

Everyone has a photographic memory. Some just don't have film.

I intend to live forever - so far, so good.

Join the Army, meet interesting people, kill them.

If Barbie is so popular, why do you have to buy her friends?

Eagles may soar, but weasels don't get sucked into jet engines.

24 hours in a day ... 24 beers in a case...coincidence?

Dancing is a perpendicular expression of a horizontal desire.

Boycott shampoo! Demand the REAL poo!

Who is General Failure and why is he reading my hard disk?

What happens if you get scared half to death twice?

Why do psychics have to ask you for your name?

If at first you don't succeed, destroy all evidence that you tried.

If at first you don't succeed, then skydiving definitely isn't for you.

A conclusion is the place where you got tired of thinking.

Experience is something you don't get until just after you need it.

The severity of the itch is proportional to the reach.

To steal ideas from one person is plagiarism; to steal from many is research.

The problem with the gene pool is that there is no lifeguard.

The sooner you fall behind, the more time you'll have to catch up.

Brigadier browns off client

Brigadier Peter Foxton told the European head of EXE Technologies how he was going to make sure that EXE's project for the army succeeded. 'If the introduction was not successful then I promised him that I would introduce him personally to the business end of the British army officer's personal weapon, the Browning 9mm,' he said. 'Future suppliers to the army should be warned: the 9mm handgun is apparently ideal for employment in relationships with contractors'.

Computing 18 October 2001

(…… and I was at school with this chap! Honestly - Ed)

The 231 Rules of Survival for Evil Overlords, or Heads of Audit

Contrary to popular belief, taking over the universe is not as easy as it would appear. Still, being an Evil Overlord seems to be a good career choice, maybe even better than being a computer auditor! It pays well, there are all sorts of perks and you can set your own hours. However every Evil Overlord I've read about or seen in movies invariably gets overthrown and destroyed in the end. I've noticed that no matter whether they are barbarian lords, deranged wizards, mad scientists or alien invaders, they always seem to make the same basic mistakes every single time. With that in mind I reproduce the rules for survival below.

A prize to the first person to spot the rule that does not apply to Microsoft and the one with an important lesson for companies. Editor's decision is final. Send entries to john@lhscontrol.com.

1. My Legions of Terror will have helmets with clear plexiglass visors, not face-concealing ones.

2. My ventilation ducts will be too small to crawl through.

3. My noble half-brother whose throne I usurped will be killed, not kept anonymously imprisoned in a forgotten cell of my dungeon.

4. Shooting is not too good for my enemies.

5. The artefact which is the source of my power will not be kept on the Mountain of Despair beyond the River of Fire guarded by the Dragons of Eternity. It will be in my safe-deposit box. The same applies to the object which is my one weakness.

6. I will not gloat over my enemies' predicament before killing them.

7. When I've captured my adversary and he says, "Look, before you kill me, will you at least tell me what this is all about?" I'll say, "No." and shoot him. No, on second thought I'll shoot him, then say "No."

8. After I kidnap the beautiful princess, we will be married immediately in a quiet civil ceremony, not a lavish spectacle in three weeks' time during which the final phase of my plan will be carried out.

9. I will not include a self-destruct mechanism unless absolutely necessary. If it is necessary, it will not be a large red button labelled "Danger: Do Not Push". The big red button marked "Do Not Push" will instead trigger a spray of bullets on anyone stupid enough to disregard it. Similarly, the ON/OFF switch will not clearly be labelled as such.

10. I will not interrogate my enemies in the inner sanctum — a small hotel well outside my borders will work just as well.

11. I will be secure in my superiority. Therefore, I will feel no need to prove it by leaving clues in the form of riddles or leaving my weaker enemies alive to show they pose no threat.

12. One of my advisors will be an average five-year-old child. Any flaws in my plan that he is able to spot will be corrected before implementation.

13. All slain enemies will be cremated, or at least have several rounds of ammunition emptied into them, not left for dead at the bottom of the cliff. The announcement of their deaths, as well as any accompanying celebration, will be deferred until after the aforementioned disposal.

14. The hero is not entitled to a last kiss, a last cigarette, or any other form of last request.

15. I will never employ any device with a digital countdown. If I find that such a device is absolutely unavoidable, I will set it to activate when the counter reaches 117 and the hero is just putting his plan into operation.

16. I will never utter the sentence "But before I kill you, there's just one thing I want to know."

17. When I employ people as advisors, I will occasionally listen to their advice.

18. I will not have a son. Although his laughably under-planned attempt to usurp power would easily fail, it would provide a fatal distraction at a crucial point in time.

19. I will not have a daughter. She would be as beautiful as she was evil, but one look at the hero's rugged countenance and she'd betray her own father.

20. Despite its proven stress-relieving effect, I will not indulge in maniacal laughter. When so occupied, it's too easy to miss unexpected developments that a more attentive individual could adjust to accordingly.

21. I will hire a talented fashion designer to create original uniforms for my Legions of Terror, as opposed to some cheap knock-offs that make them look like Nazi stormtroopers, Roman footsoldiers, or savage Mongol hordes. All were eventually defeated and I want my troops to have a more positive mind-set.

22. No matter how tempted I am with the prospect of unlimited power, I will not consume any energy field bigger than my head.

23. I will keep a special cache of low-tech weapons and train my troops in their use. That way – even if the heroes manage to neutralise my power generator and/or render the standard-issue energy weapons useless – my troops will not be overrun by a handful of savages armed with spears and rocks.

24. I will maintain a realistic assessment of my strengths and weaknesses. Even though this takes some of the fun out of the job, at least I will never utter the line "No, this cannot be! I AM INVINCIBLE!!!" (After that, death is usually instantaneous.)

25. No matter how well it would perform, I will never construct any sort of machinery which is completely indestructible except for one small and virtually inaccessible vulnerable spot.

26. No matter how attractive certain members of the rebellion are, there is probably someone just as attractive who is not desperate to kill me. Therefore, I will think twice before ordering a prisoner sent to my bedchamber.

27. I will never build only one of anything important. All important systems will have redundant control panels and power supplies. For the same reason I will always carry at least two fully loaded weapons at all times.

28. My pet monster will be kept in a secure cage from which it cannot escape and into which I could not accidentally stumble.

29. I will dress in bright and cheery colours, and so throw my enemies into confusion.

30. All bumbling conjurers, clumsy squires, no-talent bards, and cowardly thieves in the land will be pre-emptively put to death. My foes will surely give up and abandon their quest if they have no source of comic relief.

31. All naive, busty tavern wenches in my realm will be replaced with surly, world-weary waitresses who will provide no unexpected

reinforcement and/or romantic subplot for the hero or his sidekick.

32. I will not fly into a rage and kill a messenger who brings me bad news just to illustrate how evil I really am. Good messengers are hard to come by.

33. I won't require high-ranking female members of my organisation to wear a stainless-steel bustier. Morale is better with a more casual dress-code. Similarly, outfits made entirely from black leather will be reserved for formal occasions.

34. I will not turn into a snake. It never helps.

35. I will not grow a goatee. In the old days they made you look diabolic. Now they just make you look like a disaffected member of Generation X.

36. I will not imprison members of the same party in the same cell block, let alone the same cell. If they are important prisoners, I will keep the only key to the cell door on my person instead of handing out copies to every bottom-rung guard in the prison.

37. If my trusted lieutenant tells me my Legions of Terror are losing a battle, I will believe him. After all, he's my trusted lieutenant.

38. If an enemy I have just killed has a younger sibling or offspring anywhere, I will find them and have them killed immediately, instead of waiting for them to grow up harbouring feelings of vengeance towards me in my old age.

39. If I absolutely must ride into battle, I will certainly not ride at the forefront of my Legions of Terror, nor will I seek out my opposite number among his army.

40. I will be neither chivalrous nor sporting. If I have an unstoppable superweapon, I will use it as early and as often as possible instead of keeping it in reserve.

41. Once my power is secure, I will destroy all those pesky time-travel devices.

42. When I capture the hero, I will make sure I also get his dog, monkey, ferret, or whatever sickeningly cute little animal capable of untying ropes and filching keys happens to follow him around.

43. I will maintain a healthy amount of scepticism when I capture the beautiful rebel and she claims she is attracted to my power and good looks and will gladly betray her companions if I just let her in on my plans.

44. I will only employ bounty hunters who work for money. Those who work for the pleasure of the hunt tend to do dumb things like even the odds to give the other guy a sporting chance.

45. I will make sure I have a clear understanding of who is responsible for what in my organisation. For example, if my general screws up I will not draw my weapon, point it at him, say "And here is the price for failure," then suddenly turn and kill some random underling.

46. If an advisor says to me "My liege, he is but one man. What can one man possibly do?", I will reply "This." and kill the advisor.

47. If I learn that a callow youth has begun a quest to destroy me, I will slay him while he is still a callow youth instead of waiting for him to mature.

48. I will treat any beast which I control through magic or technology with respect and kindness. Thus if the control is ever broken, it will not immediately come after me for revenge.

49. If I learn the whereabouts of the one artefact which can destroy me, I will not send all my troops out to seize it. Instead I will send them out to seize something else and quietly put a Want-Ad in the local paper.

50. My main computers will have their own special operating system that will be completely incompatible with standard IBM and Macintosh powerbooks.

51. If one of my dungeon guards begins expressing concern over the conditions in the beautiful princess' cell, I will immediately transfer him to a less people-oriented position.

52. I will hire a team of board-certified architects and surveyors to examine my castle and inform me of any secret passages and abandoned tunnels that I might not know about.

53. If the beautiful princess that I capture says "I'll never marry you! Never, do you hear me, NEVER!!!", I will say "Oh well" and kill her.

54. I will not strike a bargain with a demonic being then attempt to double-cross it simply because I feel like being contrary.

55. The deformed mutants and odd-ball psychotics will have their place in my Legions of Terror. However before I send them out on important covert missions that require tact and subtlety, I will first see if there is anyone else equally qualified who would attract less attention.

56. My Legions of Terror will be trained in basic marksmanship. Any who cannot learn to hit a man-sized target at 10 metres will be used for target practice.

57. Before employing any captured artefacts or machinery, I will carefully read the owner's manual.

58. If it becomes necessary to escape, I will never stop to pose dramatically and toss off a one-liner.

59. I will never build a sentient computer smarter than I am.

60. My five-year-old child advisor will also be asked to decipher any code I am thinking of using. If he breaks the code in under 30 seconds, it will not be used. Note: this also applies to passwords.

61. If my advisors ask "Why are you risking everything on such a mad scheme?", I will not proceed until I have a response that satisfies them.

62. I will design fortress hallways with no alcoves or protruding structural supports which intruders could use for cover in a firefight.

63. Bulk trash will be disposed of in incinerators, not compactors. And they will be kept hot, with none of that nonsense about flames going through accessible tunnels at predictable intervals.

64. I will see a competent psychiatrist and get cured of all extremely unusual phobias and bizarre compulsive habits which could prove to be a disadvantage.

65. If I must have computer systems with publicly available terminals, the maps they display of my complex will have a room clearly marked as the Main Control Room. That room will be the Execution Chamber. The actual main control room will be marked as Sewage Overflow Containment.

66. My security keypad will actually be a fingerprint scanner. Anyone who watches someone press a sequence of buttons or dusts the pad for fingerprints then subsequently tries to enter by repeating that sequence will trigger the alarm system.

67. No matter how many shorts we have in the system, my guards will be instructed to treat every surveillance camera malfunction as a full-scale emergency.

68. I will spare someone who saved my life sometime in the past. This is only reasonable as it encourages others to do so. However, the offer is good one time only. If they want me to spare them again, they'd better save my life again.

69. All midwives will be banned from the realm. All babies will be

delivered at state-approved hospitals. Orphans will be placed in foster-homes, not abandoned in the woods to be raised by creatures of the wild.

70. When my guards split up to search for intruders, they will always travel in groups of at least two. They will be trained so that if one of them disappears mysteriously while on patrol, the other will immediately initiate an alert and call for backup, instead of quizzically peering around a corner.

71. If I decide to test a lieutenant's loyalty and see if he/she should be made a trusted lieutenant, I will have a crack squad of marksmen standing by in case the answer is no.

72. If all the heroes are standing together around a strange device and begin to taunt me, I will pull out a conventional weapon instead of using my unstoppable superweapon on them.

73. I will not agree to let the heroes go free if they win a rigged contest, even though my advisors assure me it is impossible for them to win.

74. When I create a multimedia presentation of my plan designed so that my five-year-old advisor can easily understand the details, I will not label the disk "Project Overlord" and leave it lying on top of my desk.

75. I will instruct my Legions of Terror to attack the hero en masse, instead of standing around waiting while members break off and attack one or two at a time.

76. If the hero runs up to my roof, I will not run up after him and struggle with him in an attempt to push him over the edge. I will also not engage him at the edge of a cliff. (In the middle of a rope-bridge over a river of molten lava is not even worth considering.)

77. If I have a fit of temporary insanity and decide to give the hero the chance to reject a job as my trusted lieutenant, I will retain enough sanity to wait until my current trusted lieutenant is out of earshot before making the offer.

78. I will not tell my Legions of Terror "And he must be taken alive!" The command will be "And try to take him alive if it is reasonably practical."

79. If my doomsday device happens to come with a reverse switch, as soon as it has been employed it will be melted down and made into limited-edition commemorative coins.

80. If my weakest troops fail to eliminate a hero, I will send out my best troops instead of wasting time with progressively stronger ones as he gets closer and closer to my fortress.

81. If I am fighting with the hero atop a moving platform, have disarmed him, and am about to finish him off and he glances behind me and drops flat, I too will drop flat instead of quizzically turning around to find out what he saw.

82. I will not shoot at any of my enemies if they are standing in front of the crucial support beam to a heavy, dangerous, unbalanced structure.

83. If I'm eating dinner with the hero, put poison in his goblet, then have to leave the table for any reason, I will order new drinks for both of us instead of trying to decide whether or not to switch with him.

84. I will not have captives of one sex guarded by members of the opposite sex.

85. I will not use any plan in which the final step is horribly complicated, e.g. "Align the 12 Stones of Power on the sacred altar then activate the medallion at the moment of total eclipse." Instead it will be more along the lines of "Push the button."

86. I will make sure that my doomsday device is up to code and properly grounded.

87. My vats of hazardous chemicals will be covered when not in use. Also, I will not construct walkways above them.

88. If a group of henchmen fail miserably at a task, I will not berate them for incompetence then send the same group out to try the task again.

89. After I captures the hero's superweapon, I will not immediately disband my legions and relax my guard because I believe whoever holds the weapon is unstoppable. After all, the hero held the weapon and I took it from him.

90. I will not design my Main Control Room so that every workstation is facing away from the door.

91. I will not ignore the messenger that stumbles in exhausted and obviously agitated until my personal grooming or current entertainment is finished. It might actually be important.

92. If I ever talk to the hero on the phone, I will not taunt him. Instead I will say this his dogged perseverance has given me new insight on the futility of my evil ways and that if he leaves me alone for a few months of quiet contemplation I will likely return to the path of righteousness. (Heroes are incredibly gullible in this regard.)

93. If I decide to hold a double execution of the hero and an underling who failed or betrayed me, I will see to it that the hero is scheduled to go first.

94. When arresting prisoners, my guards will not allow them to stop and grab a useless trinket of purely sentimental value.

95. My dungeon will have its own qualified medical staff complete with bodyguards. That way if a prisoner becomes sick and his cellmate tells the guard it's an emergency, the guard will fetch a trauma team instead of opening up the cell for a look.

96. My door mechanisms will be designed so that blasting the control panel on the outside seals the door and blasting the control panel on the inside opens the door, not vice versa.

97. My dungeon cells will not be furnished with objects that contain reflective surfaces or anything that can be unravelled.

98. If an attractive young couple enters my realm, I will carefully monitor their activities. If I find they are happy and affectionate, I will ignore them. However if circumstance have forced them together against their will and they spend all their time bickering and criticising each other except during the intermittent occasions when they are saving each others' lives at which point there are hints of sexual tension, I will immediately order their execution.

99. Any data file of crucial importance will be padded to 1.45Mb in size.

100. I will not order my trusted lieutenant to kill the infant who is destined to overthrow me — I'll do it myself.

101. I will not waste time making my enemy's death look like an accident — I'm not accountable to anyone and my other enemies wouldn't believe it.

102. I will make it clear that I do know the meaning of the word "mercy"; I simply choose not show them any.

103. My undercover agents will not have tattoos identifying them as members of my organisation, nor will they be required to wear military boots or adhere to any other dress codes.

104. I will design all doomsday machines myself. If I must hire a mad scientist to assist me, I will make sure that he is sufficiently twisted to never regret his evil ways and seek to undo the damage he's caused.

105. If my supreme command centre comes under attack, I will immediately flee to safety in my prepared escape pod and direct the defences from there. I will not wait until the troops break into my inner sanctum to attempt this.

106. Even though I don't really care because I plan on living forever, I will hire engineers who are able to build me a fortress sturdy enough that, if I am slain, it won't tumble to the ground for no good structural reason.

107. Any and all magic and/or technology that can miraculously resurrect a secondary character who has given up his/her life through self sacrifice will be outlawed and destroyed.

108. I will see to it that plucky young lads/lasses in strange clothes and with the accent of an outlander shall REGULARLY climb some monument in the main square of my capital and denounce me, claim to know the secret of my power, rally the masses to rebellion, etc. That way, the citizens will be jaded in case the real thing ever comes along.

109. I will not employ devious schemes that involve the hero's party getting into my inner sanctum before the trap is sprung.

110. I will offer oracles the choice of working exclusively for me or being executed.

111. I will not rely entirely upon "totally reliable" spells that can be neutralised by relatively inconspicuous talismans.

112. I will make the main entrance to my fortress standard-sized. While elaborate 60-foot high double-doors definitely impress the masses, they are hard to close quickly in an emergency.

113. I will never accept a challenge from the hero.

114. I will not engage an enemy single-handedly until all my soldiers are dead.

115. If I capture the hero's starship, I will keep it in the landing bay with the ramp down, only a few token guards on duty and a ton of explosives set to go off as soon as it clears the blast-range.

116. No matter how much I want revenge, I will never order an underling "Leave him. He's mine!"

117. If I have equipment which performs an important function, it will not be activated by a lever that someone could trigger by accidentally falling on when fatally wounded.

118. I will not attempt to kill the hero by placing a venomous creature in his room. It will just wind up accidentally killing one of my clumsy henchmen instead.

119. Since nothing is more irritating than a hero defeating you with basic maths skills, all of my personal weapons will be modified to fire one more shot than the standard issue.

120. If I come into possession of an artefact which can only be used by the pure of heart, I will not attempt to use it regardless.

121. The gun turrets on my fortress will not rotate enough so that they may direct fire inward or at each other.

122. If I decide to hold a contest of skill open to the general public, contestants will be required to remove their hooded cloaks and shave their beards before entering.

123. Prior to kidnapping an older male scientist and forcing him to work for me, I will investigate his offspring and make sure that he has neither a beautiful but naive daughter who is willing to risk anything to get him back, nor an estranged son who works in the same field but had a falling-out with his father many years ago.

124. Should I actually decide to kill the hero in an elaborate escape-proof death-trap room (water filling up, sand pouring down, walls converging, etc.) I will not leave him alone five-to-ten minutes prior to "imminent" death, but will instead (finding a vantage point or monitoring camera) stick around and enjoy watching my adversary's demise.

125. Rather than having only one secret escape pod, which the hero can easily spot and follow, I'll simultaneously launch a few dozen decoys to throw him off track.

126. Prison guards will have their own cantina featuring a wide variety of tasty treats that will deliver snacks to the guards while on duty. The guards will also be informed that accepting food or drink from any other source will result in execution.

127. I will not employ robots as agents of destruction if there is any possible way that they can be re-programmed or if their battery packs are externally mounted and easily removable.

128. Despite the delicious irony, I will not force two heroes to fight each other in the arena.

129. All members of my Legions of Terror will have professionally tailored uniforms. If the hero knocks a soldier unconscious and steals the uniform, the poor fit will give him away.

130. I will never place the key to a cell just out of a prisoner's reach.

131. Before appointing someone as my trusted lieutenant, I will conduct a thorough background investigation and security clearance.

132. If I find my beautiful consort with access to my fortress has been associating with the hero, I'll have her executed. It's regrettable, but new consorts are easier to get than new fortresses and maybe the next one will pay attention at the orientation meeting.

133. If I am escaping in a large truck and the hero is pursuing me in a small Italian sports car, I will not wait for the hero to pull up along side of me and try to force him off the road as he attempts to climb aboard. Instead I will slam on the brakes when he's directly behind me. (A rudimentary knowledge of physics can prove quite useful.)

134. My doomsday machine will have a highly-advanced technological device called a capacitor in case someone inconveniently pulls the plug at the last second. (If I have access to REALLY advanced technology, I will include a back-up device known as a battery.)

135. If I build a bomb, I will simply remember which wire to cut if it has to be deactivated and make every wire red.

136. Before spending available funds on giant gargoyles, gothic arches, or other cosmetically intimidating pieces of architecture, I will see if there are any valid military expenditures that could use the extra budget.

137. The passageways to and within my domain will be well-lit with fluorescent lighting. Regrettably, the spooky atmosphere will be lost, but my security patrols will be more effective.

138. If I'm sitting in my camp, hear a twig snap, start to investigate, then encounter a small woodland creature, I will send out some scouts anyway just to be on the safe side. (If they disappear into the foliage, I will not send out another patrol; I will break out the napalm.)

139. I will instruct my guards when checking a cell that appears empty to look for the chamber pot. If the chamber pot is still there, then the prisoner has escaped and they may enter and search for clues. If the chamber pot is not there, then either the prisoner is perched above the lintel waiting to strike them with it or else he decided to take it as a souvenir (in which case he is obviously deeply disturbed and poses no threat). Either way, there's no point in entering.

140. As an alternative to not having children, I will have lots of

children. My sons will be too busy jockeying for position to ever be a real threat, and the daughters will all sabotage each other's attempts to win the hero.

141. If I have children and subsequently grandchildren, I will keep my three-year-old granddaughter near me at all times. When the hero enters to kill me, I will ask him to first explain to her why it is necessary to kill her beloved grandpa. When the hero launches into an explanation of morality way over her head, that will be her cue to pull the lever and send him into the pit of crocodiles. After all, small children like crocodiles almost as much as Evil Overlords and it's important to spend quality time with the grandkids.

142. If one of my daughters actually manages to win the hero and openly defies me, I will congratulate her on her choice, declare a national holiday to celebrate the wedding, and proclaim the hero my heir. This will probably be enough to break up the relationship. If not, at least I am assured that no hero will attack my Legions of Terror when they are holding a parade in his honour.

143. I will order my guards to stand in a line when they shoot at the hero so he cannot duck and have them accidentally shoot each other. Also, I will order some to aim above, below, and to the sides so he cannot jump out of the way.

144. My dungeon cell decor will not feature exposed pipes. While they add to the gloomy atmosphere, they are good conductors of vibrations and a lot of prisoners know Morse code.

145. If my surveillance reports any un-manned or seemingly innocent ships found where they are not supposed to be, they will be immediately vapourised instead of brought in for salvage.

146. I will classify my lieutenants in three categories: untrusted, trusted, and completely trusted. Promotion to the third category will be awarded posthumously.

147. Before ridiculing my enemies for wasting time on a device to stop me that couldn't possibly work, I will first acquire a copy of the schematics and make sure that in fact it couldn't possibly work.

148. Ropes supporting various fixtures will not be tied next to open windows or staircases, and chandeliers will be hung way at the top of the ceiling.

149. I will provide funding and research to develop tactical and strategic weapons covering a full range of needs so my choices are not limited to "hand to hand combat with swords" and "blow up the planet".

150. I will not set myself up as a god. That perilous position is reserved for my trusted lieutenant.

151. I will instruct my fashion designer that when it comes to accessorising, second-chance body armour goes well with every outfit.

152. My Legions of Terror will be an equal-opportunity employer. Conversely, when it is prophesied that no man can defeat me, I will keep in mind the increasing number of non-traditional gender roles.

153. I will instruct my Legions of Terror in proper search techniques. In particular, if they are searching for escapees and someone shouts, "Quick! They went that way!", they must first ascertain the identity of this helpful informant before dashing off in hot pursuit.

154. If I know of any heroes in the land, I will not under any circumstance kill their mentors, teachers, and/or best friends.

155. If I have the hero and his party trapped, I will not wait until my Superweapon charges to finish them off if more conventional means are available.

156. Whenever plans are drawn up that include a time-table, I'll post-date the completion 3 days after it's actually scheduled to occur and not worry too much if they get stolen.

157. I will exchange the labels on my folder of top-secret plans and my folder of family recipes. Imagine the hero's surprise when he decodes the stolen plans and finds instructions for Grandma's Potato Salad.

158. If I burst into rebel headquarters and find it deserted except for an odd, blinking device, I will not walk up and investigate; I'll run like hell.

159. Before being accepted into my Legions of Terror, potential recruits will have to pass peripheral vision and hearing tests, and be able to recognise the sound of a pebble thrown to distract them.

160. I will occasionally vary my daily routine and not live my life in a rut. For example, I will not always take a swig of wine or ring a giant gong before finishing off my enemy.

161. If I steal something very important to the hero, I will not put it on public display.

162. When planning an expedition, I will choose a route for my forces that does not go through thick, leafy terrain conveniently located near the rebel camp.

163. I will hire one hopelessly stupid and incompetent lieutenant, but make sure that he is full of misinformation when I send him to capture the hero.

164. As an equal-opportunity employer, I will have several hearing-impaired body-guards. That way if I wish to speak confidentially with someone, I'll just turn my back so the guards can't read my lips instead of sending all of them out of the room.

165. If the rebels manage to trick me, I will make a note of what they did so that I do not keep falling for the same trick over and over again.

166. If I am recruiting to find someone to run my computer systems, and my choice is between the brilliant programmer who's head of the world's largest international technology conglomerate and an obnoxious 15-year-old dork who's trying to impress his dream girl, I'll take the brat and let the hero get stuck with the genius.

167. I will plan in advance what to do with each of my enemies if they are captured. That way, I will never have to order someone to be tied up while I decide his fate.

168. If I have massive computer systems, I will take at least as many precautions as a small business and include things such as virus-scans and firewalls.

169. I will be an equal-opportunity despot and make sure that terror and oppression is distributed fairly, not just against one particular group that will form the core of a rebellion.

170. I will not locate a base in a volcano, cave, or any other location where it would be ridiculously easy to bypass security by rappelling down from above.

171. I will allow guards to operate under a flexible work schedule. That way if one is feeling sleepy, he can call for a replacement, punch out, take a nap, and come back refreshed and alert to finish out his shift.

172. Although it would provide amusement, I will not confess to the hero's rival that I was the one who committed the heinous act for which he blames the hero.

173. If I am dangling over a precipice and the hero reaches his hand down to me, I will not attempt to pull him down with me. I will allow him to rescue me, thank him properly, then return to the safety of my fortress and order his execution.

174. I will have my fortress exorcised regularly. Although ghosts in

the dungeon provide an appropriate atmosphere, they tend to provide valuable information once placated.

175. I will add indelible dye to the moat. It won't stop anyone from swimming across, but even dim-witted guards should be able to figure out when someone has entered in this fashion.

176. If a scientist with a beautiful and unmarried daughter refuses to work for me, I will not hold her hostage. Instead, I will offer to pay for her future wedding and her children's college tuition.

177. If I have the hero cornered and am about to finish him off and he says "Look out behind you!!" I will not laugh and say "You don't expect me to fall for that old trick, do you?" Instead I will take a step to the side and half turn. That way I can still keep my weapon trained on the hero, I can scan the area behind me, and if anything was heading for me it will now be heading for him.

178. I will not outsource core functions.

179. If I ever build a device to transfer the hero's energy into me, I will make sure it cannot operate in reverse.

180. I will decree that all hay be shipped in tightly-packed bales. Any wagonload of loose hay attempting to pass through a checkpoint will be set on fire.

181. I will not hold any sort of public celebration within my castle walls. Any event open to members of the public will be held down the road in the festival pavilion.

182. Before using any device which transfers energy directly into my body, I will install a surge suppressor.

183. I will hire a drama coach. The hero will think it must be a case of mistaken identity when confronted by my Minnesota accent (if everyone sounds American) or my Cornwall accent (if everyone sounds British).

184. If I capture an enemy known for escaping via ingenious and fantastic little gadgets, I will order a full cavity search and confiscate all personal items before throwing him in my dungeon.

185. I will not devise any scheme in which Part A consists of tricking the hero into unwittingly helping me and Part B consists of laughing at him then leaving him to his own devices.

186. I will not hold lavish banquets in the middle of a famine. The good PR among the guests doesn't make up for the bad PR among the masses.

187. I will funnel some of my ill-gotten gains into urban renewal projects. Although slums add a quaint and picturesque quality to any city, they too often contain unexpected allies for heroes.

188. I will never tell the hero "Yes I was the one who did it, but you'll never be able to prove it to that incompetent old fool." Chances are, that incompetent old fool is standing behind the curtain.

189. If my mad scientist/wizard tells me he has almost perfected my Superweapon but it still needs more testing, I will wait for him to complete the tests. No one ever conquered the world using a beta version.

190. I will not appoint a relative to my staff of advisors. Not only is nepotism the cause of most breakdowns in policy, but it also causes trouble with the EEOC.

191. If I appoint someone as my consort, I will not subsequently inform her that she is being replaced by a younger, more attractive woman.

192. If I am using the hero's girlfriend as a hostage and am holding her at the point of imminent death when confronting the hero, I will focus on her and not him. He won't try anything with his true love held hostage. On the other hand, the fact that she has been weak, slow-witted, naive and generally useless up to this point has no bearing on her actions at the moment of dramatic climax.

193. I will make several ludicrously erroneous maps to secret passages in my fortress and hire travellers to entrust them to aged hermits.

194. I will not use hostages as bait in a trap. Unless you're going to use them for negotiation or as human shields, there's no point in taking them.

195. I will hire an expert marksman to stand by the entrance to my fortress. His job will be to shoot anyone who rides up to challenge me.

196. I will explain to my Legions of Terror that guns are ranged weapons and swords are not. Anyone who attempts to throw a sword at the hero or club him with a gun will be summarily executed.

197. I will remember that any vulnerabilities I have are to be revealed strictly on a need-to-know basis. I will also remember that no one needs to know.

198. I will not make alliances with those more powerful than myself. Such a person would only double-cross me in my moment of glory. I will make alliances with those less powerful than myself. I will then double-cross them in their moment of glory.

199. During times of peace, my Legions of Terror will not be permitted to lie around drinking mead and eating roast boar. Instead they will be required to obey my dietician and my aerobics instructor.

200. All giant serpents acting as guardians in underground lakes will be fitted with sports goggles to prevent eye injuries.

201. All crones with the ability to prophesy will be given free facelifts, permanents, manicures, and Donna Karan wardrobes. That should pretty well destroy their credibility.

202. I will not employ an evil wizard if he has a sleazy mustache.

203. I will hire an entire squad of blind guards. Not only is this in keeping with my status as an equal opportunity employer, but it will come in handy when the hero becomes invisible or douses my only light source.

204. All repair work will be done by an in-house maintenance staff. Any alleged "repairmen" who show up at the fortress will be escorted to the dungeon.

205. When my Legions of Terror park their vehicle to do reconnaissance on foot, they will be instructed to employ a Crook Lock.

206. Employees will have conjugal visit trailers which they may use provided they call in a replacement and sign out on the timesheet. Given this, anyone caught making out in a closet while leaving their station unmonitored will be shot.

207. Members of my Legion of Terror will attend seminars on Sensitivity Training. It's good public relations for them to be kind and courteous to the general population when not actively engaged in sowing chaos and destruction.

208. I will not, under any circumstances, marry a woman I know to be a faithless, conniving, back-stabbing witch simply because I am absolutely desperate to perpetuate my family line. Of course, we can still date.

209. All guest-quarters will be bugged and monitored so that I can keep track of what the visitors I have for some reason allowed to roam about my fortress are actually plotting.

210. If my chief engineer displeases me, he will be shot, not imprisoned in the dungeon or beyond the traps he helped design.

211. I will not send out battalions composed wholly of robots or skeletons against heroes who have qualms about killing living beings.

212. I will not wear long, heavy cloaks. While they certainly make a bold fashion statement, they have an annoying tendency to get caught in doors or tripped over during an escape.

213. If a malignant being demands a sacrificial victim have a particular quality, I will check to make sure said victim has this quality immediately before the sacrifice and not rely on earlier results. (Especially if the quality is virginity and the victim is the hero's girlfriend.)

214. If I ever MUST put a digital timer on my doomsday device, I will buy one free from quantum mechanical anomalies. So many brands on the market keep perfectly good time while you're looking at them, but whenever you turn away for a couple minutes then turn back, you find that the countdown has progressed by only a few seconds.

215. If my Legions of Terror are defeated in a battle, I will quietly withdraw and regroup instead of launching a haphazard mission to assassinate the hero.

216. If I'm wearing the key to the hero's shackles around my neck and his former girlfriend now volunteers to become my mistress and we are all alone in my bedchamber on my bed and she offers me a goblet of wine, I will politely decline the offer.

217. I will not pick up a glowing ancient artefact and shout "Its power is now mine!!!" Instead I will grab some tongs, transfer it to a hazardous materials container, and transport it back to my lab for study.

218. I will be selective in the hiring of assassins. Anyone who attempts to strike down the hero the first instant his back is turned will not even be considered for the job.

219. Whatever my one vulnerability is, I will fake a different one. For example, ordering all mirrors removed from the palace, screaming and flinching whenever someone accidentally holds up a mirror, etc. In the climax when the hero whips out a mirror and thrusts it at my face, my reaction will be "Hmm..I think I need a shave."

220. My force-field generators will be located inside the shield they generate.

221. I reserve the right to execute any henchmen who appear to be a little too intelligent, powerful, or devious. However if I do so, I will not at some subsequent point shout "Why am I surrounded by these incompetent fools?!"

222. I will install a fire extinguisher in every room — three, if the room contains vital equipment or volatile chemicals.

223. I will build machines which simply fail when overloaded, rather than wipe out all nearby henchmen in an explosion or worse yet set off a chain reaction. I will do this by using devices known as "surge protectors".

224. I will explain to my guards that most people have their eyes in the front of their heads and thus while searching for someone it makes little sense to draw a weapon and slowly back down the hallway.

225. I will have a staff of competent detectives handy. If I learn that someone in a certain village is plotting against me, I will have them find out who rather than wipe out the entire village in a pre-emptive strike.

226. I will never bait a trap with genuine bait.

227. If the hero claims he wishes to confess in public or to me personally, I will remind him that a notarised deposition will serve just as well.

228. If I have several diabolical schemes to destroy the hero, I will set all of them in motion at once rather than wait for them to fail and launch them successively.

229. I will not procrastinate regarding any ritual granting immortality.

230. Mythical guardians will be instructed to ask visitors name, purpose of visit, and whether they have an appointment instead of ancient riddles.

231. Finally, to keep my subjects permanently locked in a mindless trance, I will provide each of them with free unlimited Internet access.

*please note that Evil Overlord is an Equal Opportunity Position; feel free to impose the gender of your choice on any of the people/entities mentioned above. After all, you're the boss.

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Membership Application

(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members) * £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)* £25

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15

BCS membership number: _____

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).

Educational Establishment: _____ £10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
E-mail:
PROFESSIONAL CATEGORY: (Please circle) 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)
SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS IRMA"AND RETURN WITH THIS FORM TO

Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

IRMA
INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

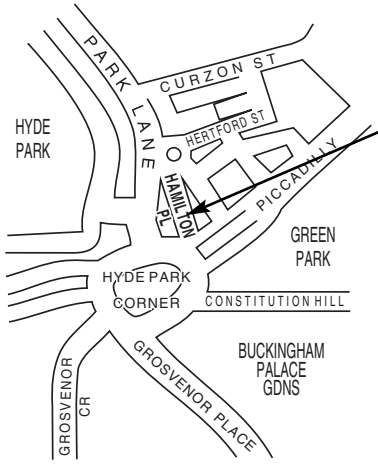
CHAIRMAN	**John Bevan**	**Audit & Computer Security Services**	**01992 582439** **john_bevan@ntlworld.com**
DEPUTY TO CHAIRMAN	**Siobhan Tracey**	**Booker plc**	**01494 442883** **siobhan.tracey@booker.co.uk**
SECRETARY	**Raghu Iyer**	**KPMG**	**020 7311 1412** **raghu.iyer@kpmg.co.uk**
TREASURER	**Mike Demetriou**	**CrestCo Ltd**	**020 7849 0000** **mike.demetriou@crestco.co.uk**
MEMBERSHIP SECRETARY	**Vacant**		
JOURNAL EDITOR	**John Mitchell**	**LHS Business Control**	**01707 851454** **john@lhscontrol.com**
WEBMASTER	**Allan Boardman**	**Goldman Sachs**	**07881 930814** **webmaster@bcs-irma.org**
SECURITY COMMITTEE LIAISON	**John Bevan**	**Audit & Computer Security Services**	**01992 582439** **john_bevan@ntlworld.com**
TECHNICAL BOARD LIAISON	**Vacant**		
TECHNICAL BRIEFINGS	**Paul Plane**	**Dai-Ichi Kangyo Bank**	**020 7283 0929 x 1222** **pplane@dkbeurope.com**
MARKETING	**Steve Pooley**	**Independent Consultant**	**01580 891036** **steve.pooley@lineone.com**
ACADEMIC RELATIONS	**David Chadwick**	**Greenwich University**	**020 8331 8509** **d.r.chadwick@greenwich.ac.uk**
LOCAL GOVENMENT LIAISON	**Peter Murray**		**01992 582105** **cass@peterm.demon.co.uk**
	Rosemary Mulley	**NabarroNathanson**	**0118 950 5640** **r.mulley@nabarro.com**

Membership Enquiries to:

Janet Cardell-Williams
49 Grangewood
Potters Bar
Herts EN6 1SL
Tel: 01707 852384
Fax: 01707 646275
Email: members.irma@bcs.org.uk
www.bcs-irma.org

Venue for

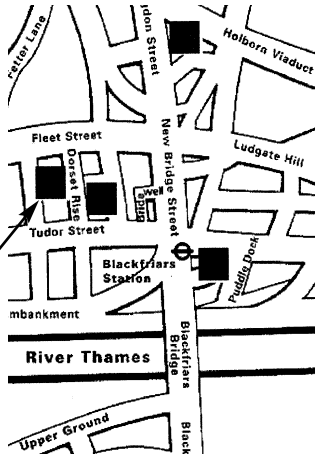
Full Day Technical Briefings



Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ

Venue for

Late Afternoon Meetings



KPMG
8 Salisbury Square
London EC4

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should either be on double spaced, single-sided A4 paper, e-mail, or in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality monochrome photograph, or electronic image.

Submission Deadlines

Spring Edition	7th February
Summer Edition	7th May
Autumn Edition	7th August
Winter Edition	7th November