Viruses and Computer Security

key*notes*

Volume 27, Number 3

contents

feature article:

viruses and computer security 4

Key*notes* on the web

Back copies of Keynotes can be found at:
http://www.york.ac.uk/services/cserv/offdocs/keynotes/

From the Editor

Happy New Year from the Computing Service, and welcome to a slim post-Christmas Keynotes.

❖❖❖

On page 3 Susanne Hodges details the background to ILIAD for University, the information literacy programme offered to incoming students, and gives feedback on this year's sessions.

❖❖❖

Page 5 sees the start of what we intend to be a regular feature as Nick Walker of the Information Desk gathers together recent top queries and points you to the solutions.

❖❖❖

Joanne Casey

Windows 95 News
by John Robinson

Applications upgrade

The applications software on the Windows 95 network was upgraded on 19th December 2000; we try not to make modifications to the applications during term-time.

We have added Perl to the Programming menu. This provides a version of Perl (ActiveState) to allow you to run Perl scripts in a DOS box, but no editing or debugging facilities. There are a number of text editors available, including the Programmer's File Editor in **Utilities | Unsupported**. The interactive Java environment JBuilder has been updated to version 4.

Reference Manager has been upgraded to version 9.5, and now allows direct export of references from the Web of Science *(http://wos.mimas.ac.uk)* to a Reference Manager database.

In Maths & Stats SAS version 8 has replaced version 6.12. Please note that during term, SPSS was updated to version 10.0.7 to avoid problems that were causing loss of data. Matlab has been updated to version 6 (as has the Unix version).

Updated systems software in classrooms

When Windows applications perform common tasks, like showing a file search dialog, they rely on code held in Dynamic Link Libraries (DLLs). Large applications also split off sub-tasks (for instance, spell checking) into DLLs, which are sometimes used in common by a number of applications. The code of DLLs changes from time to time as facilities are added or bugs fixed, and there are real problems in making sure that only the latest DLLs are used on a system with lots of applications installed. (See *http://www.york.ac.uk/services/cserv/help/win95/dll.htm* for more details).

As Windows has developed, some facilities such as DCOM (Distributed Component Object Model) and ODBC (Open DataBase Connectivity) have become added to the system. Many modern applications require these components to be installed before they will operate.

The boot volumes which hold the Windows system software for classroom PCs have recently been updated to include ODBC (setup and common drivers) and DCOM 95, and about 100 updated DLLs. What this means in practice is that applications should load faster after the daily rebuild of the PC's operating system, and that there should be no need to re-start Windows (log out and log in again) to use most common applications.

WP8 Blank documents

We have seen a number of cases of documents which appear blank in WordPerfect 8's document display screen, but which show the text (after a fashion) in the Reveal Codes screen. We have not yet found the cause of this, but it appears it can be fixed by using **Format | Page | Paper Size** and editing the current paper size, leaving it just the same as it was. There seems to be some weird interaction between WordPerfect 8, WordPerfect 9 and the printer drivers, which means that WP8 needs to be reminded that it really does know how big an A4 sheet is.

Internet Explorer

We are often asked why Internet Explorer is not installed on the Windows 95 system - it is free, after all. In fact this software makes changes to Windows itself, and, like many of Microsoft's applications is based on one-person-for-each-computer model. This means that if more than one user tries to use IE on a PC their settings tend to interfere, and there are problems if a user moves between PCs with and without IE installed. There are also problems with having both Netscape and IE on the same PC. We have investigated ways to make IE available, but have not found a way to distribute it that we would be confident we could support. But Internet Explorer will be the default web browser when Windows 2000 becomes available on the campus network.   **k***n*

Staff News
Mike Jinks

Chris Kilgour has joined us as the Web support programmer to work on the development of enhanced web-based facilities for the University, particularly in relation to development of the Intranet. Chris is a Chemistry graduate of the University which he followed with a Masters degree in Computer Science. He comes to us from Computer Science where he was a Research Associate in the Artificial Intelligence Group working on an EU-funded project with industrial collaborators.

We hope Chris will enjoy his time with us in this major development area.

The ZETOC Electronic Table of Contents Service
Sue Cumberpatch of the J B Morrell Library writes about this new service

The ZETOC service is now available to all members of the University of York. ZETOC provides access to the British Library's Electronic Table of Contents service (ETOC). The service includes an email table of contents alerting service, similar to that which was provided by the now defunct BIDS AutoJournals service.

ZETOC provides access to the contents of approximately 20,000 current journals and 16,000 conference proceedings published per year. The database of almost 15 million items covers a wide range of subject areas including science, technology, engineering, medicine, the social sciences and humanities. A list of the journal titles covered is available. The database covers from 1993 to date and is updated daily. Copies of all the articles and conference papers listed are available from the British Library Document Supply Centre.

ZETOC Alert emails the contents pages of chosen journals each time a new issue is loaded into the database.

How to access ZETOC

ZETOC is available from any PC with a suitable web browser.

On campus network PCs, select **Start | Programs | Information Resources | MIMAS**.

A link to *ZETOC* is available via the **Databases at York** page of York Information Connections at: ***http://www.york.ac.uk/ services/library/datanet.yrk/ welcome.htm*** or go direct to: ***http://zetoc.mimas.ac.uk/***.

Follow the link to ZETOC from the MIMAS home page.

A personal ATHENS account is required to access ZETOC from outside the York domain name and to use ZETOC Alert.

Searching ZETOC

The Library has produced a guide to using ZETOC, and this is available on LibWeb at: *http://www.york.ac.uk/services/ library/guides/zetoc.htm*

There is also extensive online help once you are logged into the service.

You can search using a range of terms, including title, author, ISBN, conference details, journal title, and keyword.

Saving and outputting results

Search results can be emailed to you. You can also print direct from the web browser, or copy and paste into a word processing package.

ZETOC Alert

ZETOC has a Table of Contents alerting service which emails you the contents pages of your chosen journals every time a new issue is loaded into the database. There is no limit to the number of alerts you can create, although there is a restriction to 50 journals in each Alert List. ZETOC Alert requires an ATHENS account.

Further information

For further information about ZETOC, contact Sue Cumberpatch (email: *sc17@york.ac.uk*, tel 433891) or your Subject Librarian.

Windows 2000 and Teaching Software
John Illingworth

Next Autumn Term, all being well, Computing Service PC classrooms will be running Windows 2000 rather than Windows 95. We intend to provide the same software packages as we have now, plus extras like Microsoft Office.

However we currently provide on the central servers a considerable amount of teaching software provided by departments, and clearly we can only migrate this to Windows 2000 if we are provided with suitable versions of the software. In order not to perpetuate software that is no longer used, we will only migrate software if asked to do so, and to this end we will be sending out requests to each department with software on the central systems very soon.

At the moment, the following departments have entries in the teaching software section of the central menu:

• Archaeology
• Biology
• CHE
• Chemistry
• DoFM
• Economics
• Educational Studies
• Electronics
• Health Science
• History
• Language & Liguistics
• Maths
• Medieval Studies
• Physics
• Politics
• Psychology
• Social policy
• Sociology

ILIAD for University
Sue Hodges writes about its background and gives feedback on this year's programme

In the early 1990s University of York staff in the Computing Service and Library became aware of the need to equip students with a comprehensive range of information handling skills, including retrieving, processing and presenting information in its many forms. In 1994 an Information Literacy Course Designer was appointed, whose brief was to research, design and develop materials for such a programme. The project became known as ILIAD (Information Literacy in All Departments) and was piloted in October 1995.

Since then the project has expanded into two major strands. The initial programme has been renamed as ILIAD for University and is now a large scale University wide initiative, each year raising incoming York students to a common standard of basic, transferable information handling skills to make them more effective in their studies. Although the programme is optional, most departments require the skills taught. ILIAD for the Workplace is a smaller initiative that runs throughout the year, preparing students for the world of work.

In Autumn 2000, registration forms for the ILIAD for University programme were sent out to all incoming students in September. They generated much interest and, although participation rates were slightly lower than last year, 32% of first year students signed up, with over 26% taking the taught course and 5% the self-study route. This figure includes the Department of Health Studies to which, because of timetabling difficulties, a separate programme was delivered over the week beginning 2nd October.

This year the programme consisted of four sessions: Computing at York, Researching and Evaluating Information Sources, Word Processing for Academic Purposes and Presenting Information using a Computer. Due to feedback garnered from workshops held earlier in the year with tutors and previous students, more advanced exercises and key tasks were added to the workbooks. Evaluations showed that 21.5% of participants found the programme to be very good, 66.5% found it good and the remaining 12% found it acceptable. For the first time, the Researching and Evaluating Information Sources session - showing students how to search the Library catalogue and YorkWeb - proved to be the most popular session.

However, several anomalies have been highlighted this year. Firstly, some departments are now teaching skills modules that at times overlap with skills taught on the ILIAD for University programme. Thus students from those departments who have paid to take the programme may feel that they are duplicating work taught for free within their academic department. We feel more interaction with departments may be a way forward in coming years.

Secondly, increased communication and information technology teaching in schools means that the level of incoming students' IT experience is more advanced each year. Thus, although more advanced skills and exercises were added this year, 22% of students still found some parts of the course too easy - 5% more than last year. Yet to make the programme much more advanced would take it away from its original remit of raising incoming students to a common basic level of information skills - and there is clearly still quite a large number of students entering York University with very little computing experience, who need a basic introduction to academic information literacy.

The skills that ILIAD teaches have become an important element of the learning support component of subject reviews and have contributed significantly to recent successes at York. However, the problems discussed above will need to be addressed when planning for next year's programme. Each year adds to the experience of running this large scale initiative and the programme is continually evolving to suit the changing information technology needs of incoming students.

k*n*

iliad news

Viruses and Computer Security At York
Dr Arthur Clune brings you up to date on security issues...

Computer security and 'hacking' have been in the news recently after Microsoft found that unauthorised people had been inside their system. Such incidents attract a lot of attention, but serious attacks are comparatively rare. Much more common are problems caused by computer viruses and in this article I'll describe them and some steps you can take to help prevent problems.

The common image of a virus writer is of a teenage to mid-twenties male, with poor social skills but excellent computing skills. Though there are female virus writers, this stereotype has a certain amount of truth in it. As with many forms of anti-social behaviour the appeal seems to pall for most people after a while.

By no means are all virus writers very skilled. In fact viruses are written by a wide range of people from the highly skilled with a detailed knowledge of their target system to new programmers who cause as much damage by accident as by design. The viruses themselves reflect this and the fact that virus writers' intentions range from being maliciously harmful to simply wishing to keep themselves amused. Sometimes, however, the intentions and results can disagree. For example, the Love Bug virus which caused so much damage last year was in fact a very badly written piece of software. It was evidently designed to be a stealthy virus, lying undetected on the target system. But most of the damage it caused was because it mailed itself to everyone in the target's address book and the resulting storms of email crashed servers all over the world. If it had done what its writer intended it wouldn't have sent so much mail out and might have caused far less trouble.

This type of virus is called a 'macro virus'. These are small programs that run in the programming language that is built into most modern applications. For example, a common macro virus would be an email with a Microsoft Word attachment. When you open the document, the virus runs, looks in your (Outlook) address book and emails itself to all of your contacts - as the Love Bug virus did.

Since Microsoft Office is the most common software, most macro viruses are written for Microsoft (MS) products. They do exist for other software, but to a lesser extent. As the University moves to make MS Office its supported software, these macro viruses will become more of a problem. Furthermore, the tight integration between various MS products and their operating systems (which can be very useful for the end user) means that it is easier for a virus writer to find ways to make programs such as MS Word do things that they shouldn't.

There are two things you can do to try to avoid getting a virus. Firstly, run Sophos, the virus checking software provided by the Computing Service. It will regularly check all your files for known viruses and warn you if it finds any. It will then try and get rid of them for you. If you're not running Sophos, installation instructions are available at: *http://www.york.ac.uk/services/cserv/sw/sophos/sophos_antivirus.htm*

If you have an unsupported connection, then Sophos can be downloaded from the web site. It is licensed for use on University or home computers for all staff and registered students.

Secondly, be careful about what you install on your computer. Things to be especially careful of are email attachments that are executable files (.EXE files). Don't run an attachment unless you know the sender and were expecting it. If you get an attachment that you're unsure about, save it to disk without running it (usually you can do this by right-clicking on it) . Likewise, to guard against macro viruses when you receive, for instance, a Word document in an attachment, it's safest to save the attachment to a file before opening it in Word - unless you're sure that the sender is careful. The Sophos Intercheck component (a red lightning flash in the Windows system tray) checks all new files on access. We now have a Sophos sweep on demand for the M: drive of supported PCs - look in the **Systems and Supported Utilities** menu.

In an effort to help stop the spread of email and macro viruses, the Computing Service is currently looking at ways of screening incoming email for viruses and dealing with any mail that has a virus attached. However, for the moment it's up to you to be careful with any files that you get from the internet or via email.

Desk Notes
Nick Walker of Computing Service Infodesk

The Information Desk should be your first point of contact with the Computing Service. You can email us on *infodesk@york.ac.uk* or ring extension 3838. Featured below are some of the issues which have been concerning our users recently.

Installing a virus checker
Download Sophos AntiVirus, which is licensed for use on campus and on stand alone PCs owned by University staff and students. Details may be found at:
http://www.york.ac.uk/services/cserv/sw/sophos/ sophos_antivirus.htm

Current virus alert
Many users are still experiencing problems with W32 Apology-B. Details of a fix to be implemented by competent users are available at:
http://www.york.ac.uk/ServerSupport/Liana/ News_20001113_145443.html If you have any problems, please contact the Information Desk.

Accessing your University email from home
Telnet access is not recommended for off-campus mail reading. You are advised to configure your home mail package to pick up your email. For details see:
http://www.york.ac.uk/services/cserv/docs/guides.yrk/ eguide/eguide.htm

Office 2000
This is now available to staff for purchase or upgrade under the CHEST agreement. For more information on this and other software available to purchase, see:
http://www.york.ac.uk/services/cserv/sw/ or call in to the Information Desk.

Course Registration
Since the removal of charges for Staff and Graduate Computing Service courses, we have introduced a new course registration system which speeds up the registration process. This also allows users to be placed on a reserve list if a course is full - they will be automatically informed if a place becomes available. To register for a course email or ring. The course schedule is on the web at:
http://www.york.ac.uk/services/cserv/training/

Fault reporting
The quickest way to ensure that a problem with a classroom PC is resolved is to mail the details to the Information Desk. Include the machine's number, normally found on a sticker on the monitor.

Purchasing hardware
The purchasing pages at:
http://www.york.ac.uk/services/cserv/purchase/ give information on preferred suppliers, and advice on buying for departmental and private use. The Information Desk staff can supply you with a list of various local suppliers if you're buying for private use - please note that this does not imply any recommendation.

Blocked email
The problem of blocked email can be infuriating for both sender & recipient, occasionally hindering legitimate correspondence when a reputable company's mail server is open and therefore blacklisted. Blocking takes place as a security measure against 'open mail relays', that is mail that can be sent from anywhere in the world sent to the server to be forwarded to anyone else, anywhere in the world. This device, commonly used to deliver unsolicited email - or spamming as it has become known - make it very difficult to trace & therefore take action against the sender if the mail is dangerous, in terms of a virus, or simply unwanted.

We make use of several Internet-wide blacklists to filter out unsolicited e-mail arriving for our users It is important however to remember that any measures taken to prevent the delivery of mail are done so with user security in mind and are not necessarily a reflection on the integrity of the sender.

When we reject an incoming message because of a blacklist entry our mail server returns a short customised error message. This explains that the problem concerns an open mail relay and refers the sender to the relevant web page.

If your correspondents have a problem with sending mail to the IMAP server at York they need to contact the administrator of their mail systems, advise them that their mail service is an open mail relay and direct them towards the following Internet wide databases:
ORBS - (Open Mail Behaviour Modification System)
http://www.orbs.org/
RSS - (Relay Spam Stopper database)
http://www.mail-abuse.org/rss/

They will need to upgrade or re-configure their mail server to prevent it from acting as a mail relay

(continued from overleaf)

server. Hints & tips about this for mail server packages can be found at:
*http://www.mail-abuse.org/tsi/ar-fix.html*

Following the a completion of a form from the above sites they can request that their mail system be re-tested and if their server passes as OK, their entry will be removed from the database. As an interim measure should the blacklisted organisation need more time to sort out the problem, the site can be 'whitelisted' for a short period, allowing mail to be received by us whilst still blacklisted in the Internet-wide databases. This should be requested through *postmaster@york.ac.uk,* details to include the IP address of their mail servers.

In addition we have provided the following web page for users to determine why they are having problems and advice as to a solution. To use the site correctly the user will need their numeric 'IP address'. Directions to this page are given as part of the blocked email response.
http://www.york.ac.uk/cgi-bin/mail-problems.

Crossword
Zeuss

Completed crosswords to the Computing Service by Monday 5 February. The first correct entry drawn will receive a bottle of wine.
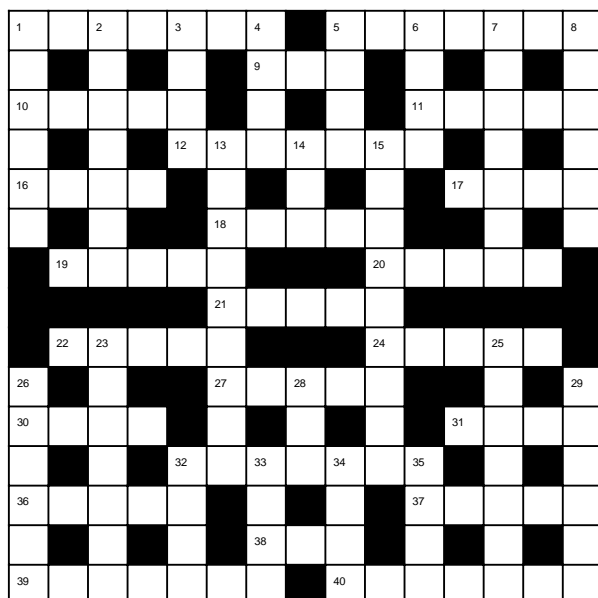
Across:

1 Fish cracked the action (7)
5 Another fish is seen to hide it (7)
9 See **38**
10 Lost 50 Kb to believe in remote connection (5)
11 Kahn's in one more time (5)
12 Sounds like mum's sister's levy is against the charge (7)
16 C'mon! Change poles and conduct (4)
17 Are all those in the place? (4)
18 Go to stay and perch on the editor (5)
19 I hear that you and nine others are bored (5)
20 Look after your information with one of these (5)
21 Two Einsteins? (5)
22 Extreme Sun (5)
24 What have they done to Bill's lovely code? (5)
27 JB's credit note is compact (5)
30 He was left sad, by being always on (4)
31 Meat in the mail? (4)
32 How many for freedom? (7)
36 VXD loses the right to store data on (5)
37 What's the location of the pirate? (5)
38, 9 Read the poem back to the sheep from memory (3, 3)
39 Naps during RIP bill, cooking the vegetable (7)
40 Full strength cat naps drive the tape (7)

Down:

1 Find Ted, etc. (6)
2 Scam the relations link, and bring together (7)
3 A tad too much information (4)
4 Damn! That dart was bad (4)
5 Cambridge college let out aEuropean (4)
6 Tempt to walk the high wire (4)
7 I'm a drag queen doing the circuit (7)
8 A charge on bad behaviour gives structure (6)
13 A browser lets you be this (9)
14 Open the Gates to the world! (3)
15 Accredit the tag's value (9)
23 IT left the user feeling stronger (7)
25 Tara installed the app to get the equipment (7)
26 Can't afford 36, climbing (6)
28 Put the class in with the jam (3)
29 Books sailing down the river (6)
32 European college head gave a DNA sample (4)
33 Search and note salesman (4)
34 Can you cope with another OS? (4)
35 Space to exchange (4)

Computing Service Address

Computing Service	Telephone:	Switchboard (01904) 430000
University of York		Direct dialling (01904) 43 followed by ext no.
Heslington	Fax:	(01904) 433740
YORK YO10 5DD	Email:	*username*@york.ac.uk

Also, try the World Wide Web: http://www.york.ac.uk/services/cserv/

Information Desk

Telephone: ext 3838
Email: *infodesk*

The Information Desk is open from 9am to 5.15pm Monday to Thursday, and 9am to 4.15pm Friday (*may be closed for training Wednesdays 2pm-3pm*), for problem solving, advice and information, fault reporting, network connections, file conversion, sales, course bookings, registration and documentation. Printed output can be collected from the lobby entrance which is open from 8am to midnight.

Computing Service Staff:

Director:	Mike Jinks	3801	*kmj1*
Departmental Secretary:	Lorraine Moor	3801	*lsm1*
Head of Infrastructure:	Robert Demaine	3808	*rld1*
Head of User Services:	John Illingworth	3803	*jji1*
Head of MIS:	Kay Mills-Hicks	2101	*kmh8*
Head of Technical Services:	Doug Moncur	3815	*dgm1*
Head of Systems:	Andrew Smith	3809	*abs4*
Operations Manager:	Brian Souter	3814	*bs1*
Head of Networking	John Mason	3813	*jrm13*
Information Officer:	Joanne Casey	3805	*jmc8*

Sue Bolton	2102	*sjb28*		Paul Hodgson	4347	*ph25*
Mike Brudenell	3811	*pmb1*		Geoff Houlton	2100	*gph2*
Lisa Burkinshaw	3818	*ljb4*		Jenny Jackson	4455	*jj5*
John Byrne	3812	*jcb1*		Chris Kilgour	4454	*crhk1*
David Chambers	3742	*dac6*		John Marsden	3832	*jpm1*
Michael Clark	3745	*mpc3*		Darren Munday	3821	*dam6*
Arthur Clune	3129	*ajc22*		Nicola Normandale	4695	*ncn1*
Paul Conacher	4346	*pac1*		Colin Rea	3817	*cr9*
Steve Downes	3741	*sd21*		Chris Reece	3807	*car7*
Debra Fayter	3839	*daf3*		John Robinson	3833	*jsr1*
Ken Finch	4452	*kf1*		Sam Scott	3817	*svs2*
Rob Fletcher	3816	*rpf1*		Daniel Shelton	4349	*ds23*
Kevin Gardner	3739	*pkg4*		Sam Vines	3749	*sccv1*
Chris Gowland	3823	*cg1*		Nick Walker	3897	*njw8*
Peter Halls	3806	*pjh1*		Timothy Willson	2123	*ftmw1*
Linda Hearn	3800	*lch8*		Mark Wilson	3826	*mw119*
Sue Hodges	3839	*sh32*		Michael Woodhead	3825	*mw28*