1966 40 YEARS OF CNL 2006

CERN COMPUTER NEWSLETTER

Volume 41 Number 1 January–March 2006

Contents

Editorial
CNL celebrates 40th birthday 1

Announcements & news
Computing featured in this month's *CERN COURIER* 3
CERN network database clean-up project begins 3
Non-Admin tackles Windows security 3
Videoconferencing with HERMES 3
Computer Centre opens to the public 3
Students invited to apply for openlab 3
EU funds EGEE-related projects 4
Tim Berners-Lee starts blog for 'semantic stuff' 4

Desktop computing
CERN enforces Web-authoring encryption to ensure security 5

LCG news
PROOF will analyse LHC data 6
Grid technology helps UNOSAT to tackle humanitarian challenges 7
Canada's TRIUMF is home to ATLAS Tier-1 centre 7

Technical briefs
A 'defence-in-depth' strategy to protect CERN's control systems 8

Conference report
US HEPiX attracts large audience 10

Information corner
Users must be suspicious when reading e-mails 11
IT database staff gain Oracle 10g certification 12
Recent changes to IT services 12
Calendar 12

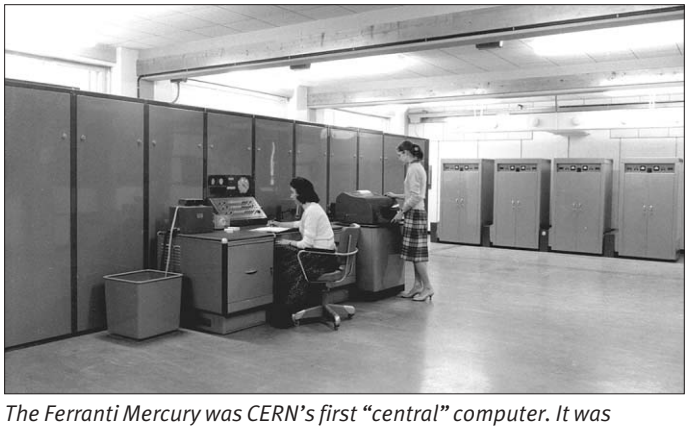
Editors Nicole Crémel and Hannelore Hämmerle, CERN IT Department, 1211 Geneva 23, Switzerland. E-mail: cnl.editor@cern.ch. Fax: +41 (22) 7668500. Web: cerncourier.com/articles/cnl.

Advisory board Wolfgang von Rüden (head of IT Department), François Grey (IT Communication team leader), Christine Sutton (*CERN Courier* editor), Tim Smith (group leader, User and Document Services).

Produced for CERN by Institute of Physics Publishing
Dirac House, Temple Back, Bristol BS1 6BE, UK. Tel: +44 (0)117 929 7481. E-mail: jo.nicholas@iop.org. Fax: +44 (0)117 920 0733. Web: iop.org.

Published by CERN IT Department

CNL celebrates 40th birthday



The Ferranti Mercury was CERN's first "central" computer. It was installed in building 2 on 30 June 1958. The Mercury's performance did not compare to the simplest of today's pocket calculators. Its clock speed was a modest 1 MHz and its RAM capacity was 2000 20-bit words.

CNL – the early years

It is 1966. The Soviet Luna 9 makes the first controlled spaceship landing on the Moon. John Lennon announces that the Beatles are more popular than Jesus. Mao Tse Tung's *Little Red Book* is published. England wins the football World Cup at Wembley Stadium. And the first *CERN Computer Newsletter* is circulated!

To celebrate *CNL's* 40th anniversary, we look back at some of the highlights and historical curiosities of the early years of computing at CERN, as reported in the newsletter.

Why was there a need for CNL?

"As computing becomes a more and more widespread and complex activity in the laboratory, the need will increase for a means to have a wider general circulation of background information about different aspects of computing activities than is possible with the present system of Computer Notices." (February 1966, from the introduction to the first issue by G R Macleod, the leader of the Data Handling division from 1964 to 1975.)

Ancestor of the Helpdesk

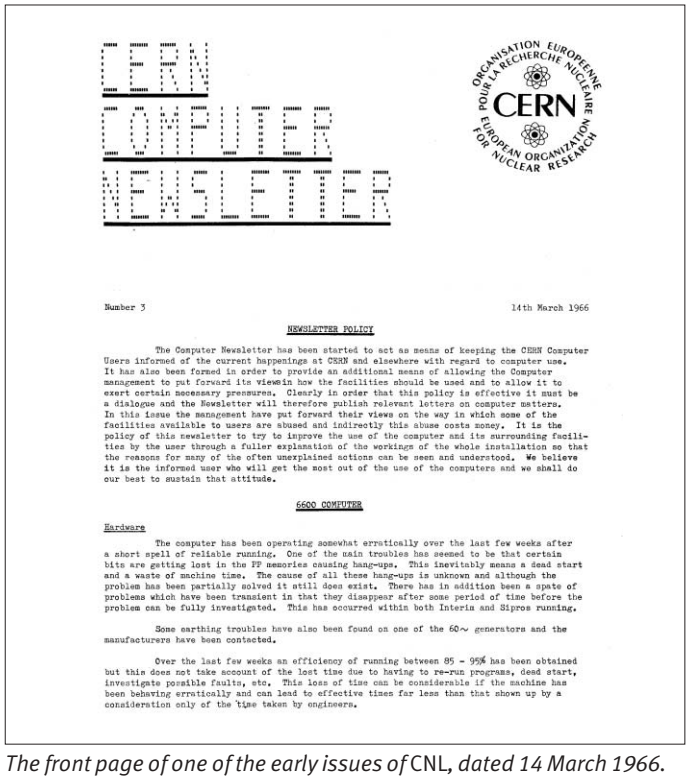
"The Enquiry Office [...] has had to cope with enquiries on both our installed machines and also to adapt themselves to the rapidly changing demands due to the running on outside computers." (March 1966)

"The principal purpose of the office is to help programmers in obtaining useful results from the computers. Advice is given on such topics as speeding up programs, better use of magnetic tapes as well as on the problems of debugging. Suspected machine faults are analysed and discussed with the CDC engineers." (February 1967)

CERN's first computer expires

"The Ferranti Mercury [...] has now been dismantled [...] The computer was the first to be installed at CERN and remained as the only machine until the arrival of the IBM 709 in 1961." (July 1966) ▷

Editorial



CERN COMPUTER NEWSLETTER

ORGANISATION EUROPÉENNE POUR LA RECHERCHE NUCLÉAIRE
CERN
EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH

Number 3 — 14th March 1966

NEWSLETTER POLICY

The Computer Newsletter has been started to act as means of keeping the CERN Computer Users informed of the current happenings at CERN and elsewhere with regard to computer use. It has also been formed in order to provide an additional means of allowing the Computer management to put forward its views in how the facilities should be used and to allow it to exert certain necessary pressures. Clearly in order that this policy is effective it must be a dialogue and the Newsletter will therefore publish relevant letters on computer matters. In this issue the management have put forward their views on the way in which some of the facilities available to users are abused and indirectly this abuse costs money. It is the policy of this newsletter to try to improve the use of the computer and its surrounding facilities by the user through a fuller explanation of the workings of the whole installation so that the reasons for many of the often unexplained actions can be seen and understood. We believe it is the informed user who will get the most out of the use of the computers and we shall do our best to sustain that attitude.

6600 COMPUTER

Hardware

The computer has been operating somewhat erratically over the last few weeks after a short spell of reliable running. One of the main troubles has seemed to be that certain bits are getting lost in the FF memories causing hang-ups. This inevitably means a dead start and a waste of machine time. The cause of all these hang-ups is unknown and although the problem has been partially solved it still does exist. There has in addition been a spate of problems which have been transient in that they disappear after some period of time before the problem can be fully investigated. This has occurred within both Interim and Sipros running.

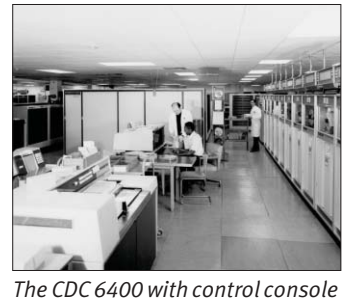
Some earthing troubles have also been found on one of the 60~ generators and the manufacturers have been contacted.

Over the last few weeks an efficiency of running between 85 - 95% has been obtained but this does not take account of the lost time due to having to re-run programs, dead start, investigate possible faults, etc. This loss of time can be considerable if the machine has been behaving erratically and can lead to effective times far less than that shown up by a consideration only of the time taken by engineers.

The front page of one of the early issues of CNL, *dated 14 March 1966.*

The newly built computer centre, building 513, as it looked in June 1972.

The CDC 3800 was used to process Swiss election data in 1967.



The CDC 6400 with control console (centre) and tape decks (right).

The end of Fortran?
"● FORTRAN: FORmula TRANslating. The most commonly used program language exists in many versions e.g. CERN Fortran.
● ALGOL: From Algorithm. A more advanced language now available on many computers but rarely efficient for production work.
● PL1: The new programming language specified by the IBM users' organization (SHARE) and IBM to supplant Fortran." (April 1966)

Un problème de traduction
"Le Comité d'Etude des Termes Techniques Français nous prie de soumettre à l'appréciation de nos lecteurs spécialisés dans le calcul automatique le choix des termes français proposés en remplacement des termes anglais *hardware* et *software* [...]

"*HARDWARE*: équipement matériel et ensemble des appareils formant une calculatrice électronique.

"*SOFTWARE*: en opposition avec le terme précèdent, désigne tout ce qui vient s'ajouter aux calculatrices électroniques pour permettre, faciliter, assouplir et accélérer le traitement de l'information.

"Cet ensemble comprend, notamment, les relèves d'un double jeu de mots en anglais. L'acception banale de *hardware* est quincaillerie et c'est par plaisanterie que ce mot est appliqué à la partie matérielle d'une calculatrice. Le mot *software* fait contraste avec *hardware* (*hard* = dur; *soft* = mou) pour désigner ce qui, en dehors du matériel, est indispensable au fonctionnement de la calculatrice.

"Traductions proposées: [...]
1) *hardware* = MATERIEL
2) *software* = PROGRAMMAIRE ou PERIGRAMME." (June 1967. Articles were sometimes written in French in the early days.)

Online in the swinging sixties
"FOCUS is the acronym for a Facility for On-line Computation and Updating Services. It is a project to give an improved computing service for the on-line users. These users are the groups who require data link connections between their own satellite computer and the large central computers." (September 1967)

CERN computing and democracy
"The following press announcement was made concerning the use of the CDC 3800 for the election data processing.

"Meyrin-Genève: un ordinateur du CERN, un CDC 3800, a effectué le dépouillement électronique des bulletins de votations des Elections fédérales suisses au Conseil national et au Conseil des Etats. Cette opération faisait partie d'un contrat entre l'Administration cantonale genevoise et l'Organisation Européenne pour la Recherche Nucléaire." (November 1967)

Not quite the Web
"ITIRC, IBM Technical Information Retrieval Center, has developed an evolutionary computerized textual information system [...] for document storage, retrieval, current awareness, dissemination, and preparation of special tools such as index listings, bulletins, KWOC, etc... This is to service within IBM, its multithousand international community of line and staff personnel." (April 1968)

GUI, seventies style
"Over the last six months there have been two additions to the types of graphics devices connected to the central computer installation. The FOCUS system has had three Tektronix T4002 storage tube displays added as terminals, and a Ferranti ARGUS 500 computer with a refreshed display, keyboard, tracker ball and light pen has been attached to the 6600. For these devices the user writes his program for the 6600 using the graphic software system GD-3 [...] the file can be returned to FOCUS where the TV command allows the user to view the output on the T4002 screen. In the latter case the user may expand a part of the picture, superpose pictures or compare frames side by side." (November 1970)

A computer centre is born
"At the Finance Committee on 12th February 1970 two adjudication papers were presented concerning the new computer building [...] The adjudications were for the air-conditioning plant, and the civil engineering work. The building will be about 75 m long by 50 m wide, with three floors above ground level and a basement, and will be built close to the new CERN restaurant on the South side of the site between the ISR and the PS." (March 1970)

"The nearly completed new computer building, building 513, which will house the CDC 7600 computer system, is located in the French site sandwiched between the new restaurant and the booster." (January 1972)

CERN network database clean-up project begins

The network database is a key element of the CERN network infrastructure. It is essential that its information is kept up to date, for security reasons and to ensure the smooth running of the network infrastructure. Over the years some of the information in the database has become obsolete; the database therefore needs to be cleaned up, for which we are requesting your help.

In the coming weeks you may receive an e-mail from Netops.database@cern.ch relating to the clean-up. If you receive such a message, it will be for one of the following reasons:

- You are responsible for or are the main user of a system for which a problem has been found.
- You have been the supervisor of a person who has now left CERN (according to the Human Resources database).
- The problem has been passed up to you because someone under your supervision has not taken the necessary action within four weeks of notification.

Just open the link that will be included in the message and follow the instructions. Thank you in advance for your help.

IT Department, Communication Systems and Network Group

- The above article was also published in *CERN Bulletin* 50–51/2005 (December 2005).

NonAdmin tackles Windows security

From 16 January, Windows XP NICE installations (both new computers installed and old computers re-installed) will no longer grant administrative privileges by default to the main user or to the person responsible for the computer.

Administrative privileges enable the user to perform administrative actions, such as installing new applications or changing system settings. Until now these privileges have been enforced each time machines are rebooted, but this risks compromising the computer every time a code from an unknown source (e.g. e-mail attachment) is executed.

To enable users to continue to install software and change system settings on their computers, a shortcut called NiceAdmin in the Start/Programs menu will offer a means of performing certain tasks that require administrative privileges, but only on demand.

Users with valid reasons to be a permanent administrator for their machine will still have this option. However, users who wish to benefit from this increased security proactively without reinstalling their computer can already sign up for the project. More information and the enrolment procedure can be found at: http://cern.ch/WinServices/docs/nonadmin.

The NICE team

Videoconferencing with HERMES

The messenger of the gods brings CERN a new service for hosting multipoint remote meetings. HERMES is operated by CERN together with IN2P3, CNRS and INSERM.

HERMES relies on a Codian 40-port Multipoint Control Unit/videoconference bridge and is similar to the ESnet ECS 88 service. It enables high-quality conferences that can be managed with great flexibility.

Current IP connectivity will be supplemented in January with ISDN (video) and traditional telephone capabilities.

The service includes advanced features such as Web streaming of conferences (using either RealPlayer or Quicktime) and individual selection of the conference display style. Soon it will also be possible to book videoconferences from the Indico interface.

Information about the service can be found at http://cern.ch/it-multimedia/HERMES.htm. (Contact videoconference-support@cern.ch.)

Thomas Baron, IT/UDS

Computer Centre opens to the public

Two more of CERN's experimental facilities have been added to the tours offered by the Visits Service. The public can now visit the COMPASS experiment and the Computer Centre.

The Computer Centre has always been a popular place to bring visitors, and the growing public awareness of CERN's Grid activities is increasing the demand. More than 1000 people passed through during CERN's open day in October 2004, and it was one of the most popular options on the site.

The first batch of guides has now been trained. During the tour, visitors will find out more about the development of the Grid and its importance to CERN and the global scientific community. Visitors will also be able to appreciate the amount of computing power required to process data from the Large Hadron Collider, by comparing their own PCs with the thousands of new desktop computers.

The Visits Service now offers seven sites. For more details, refer to http://cern.ch/visits.

Students invited to apply for openlab

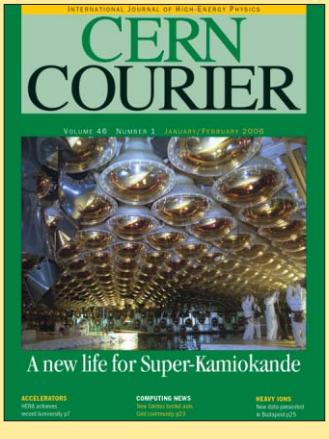
The CERN openlab student programme is open for applications from bachelor, master and Ph.D. students in computing and physics.

Successful applicants will spend two months at CERN this summer working on cutting-edge Grid-related technology projects. They will receive training in all aspects of Grids from LCG, EGEE and CERN openlab staff.

Check www.cern.ch/openlab for details. Candidates should send a CV and letter of support from a supervisor to Francois.Grey@cern.ch. The closing date for applications is 31 March.

Computing featured in this month's CERN Courier

The articles listed below appear in the January/February 2006 issue of *CERN Courier*. Full-text articles and the rest of the issue's contents are available at www.cerncourier.com.



Computing News

- **ETICS assures quality on the Grid**
EU-funded project will improve the coherence of Grid software.
- **Grid researchers get one online identity**
A new Grid federation will give scientists access to global data.
- **Python developers swap ideas**
News from the 2005 EuroPython conference in Göteborg, Sweden.
- **SC|05 showcases high-energy computing**
Grid scientists flock to Seattle.
- **CNL is 40 years old**
Early days of computing at CERN.
- **Meeting highlights Grid potential**
CERN and UNESCO host event.
- **Middleware has two important additions**
NMI-R8 eases resource security.
- **W3C improves features for transforming and querying XML**
W3C issues recommendations.

IT products and calendar

Feature articles

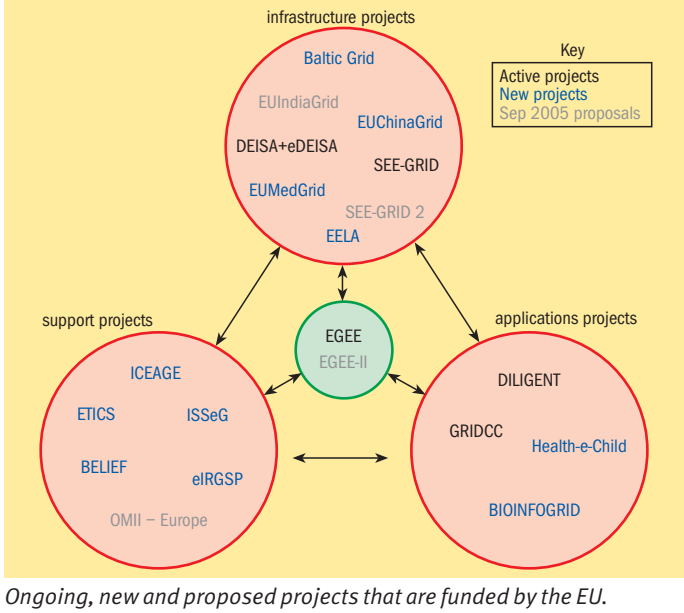
- **Tackling the challenge of lattice QCD**
Fermilab's commodity solution for lattice QCD goes online.
- **Towards a read–write Web**
Security efforts by LCG and EGEE unite the Web and the Grid.
- **Globus Toolkit upgrade aids the Grid community**
GT4 offers major improvements in terms of performance.

EU funds EGEE-related projects

One of the primary goals of the Enabling Grids for E-sciencE (EGEE) project is to integrate thematic and national Grid projects to support the rapidly emerging European Grid infrastructure. EGEE has therefore always had close relations with other Grid initiatives such as DEISA, SEE-GRID and DILIGENT.

The EU has recently funded many new projects in areas that are closely related to the work of EGEE. These projects can be sorted into three categories: infrastructure, application and support (see figure).

Infrastructure projects work in two ways: either they provide new sorts of infrastructure (such as the DEISA supercomputer Grid), or they extend existing Grid infrastructure and network capacity to new geographical regions. This regional model for infrastructure extension is now also being adopted for China, the Mediterranean area, the Baltic States and Latin America.



Ongoing, new and proposed projects that are funded by the EU.

Application projects use the Grid infrastructure to serve various goals but also help to understand the requirements of users and feed these back into the Grid development. Two new application projects, Health-e-Child (computationally intensive research in paediatrics) and BIOINFOGRID (bioinformatics), will soon come online.

Support projects include initiatives that will contribute to the development of the Grid, enhancing the impact and effectiveness of infrastructure and application projects. The e-Infrastructures Reflection Group (e-IRG) receives support in the form of the e-IRG Support Project. ISSeG (led by CERN) will work in the area of site security for Grid computing. BELIEF will help European Grid projects to develop contacts worldwide with industry, while the ICEAGE project aims to advance education about the Grid. ETICS (led by CERN), will bring together facilities for software configuration, integration, testing and benchmarking to enable developers to ensure the quality and compatibility of their products. (See also "ETICS assures quality on the Grid" (p13) in the Jan/Feb issue of *CERN Courier*.)

Tim Berners-Lee starts blog for 'semantic stuff'

Submitted by Tim Berners-Lee 12 December 2005 at http://dig.csail.mit.edu/breadcrumbs/blog/4: "In 1989 one of the main objectives of the WWW was to be a space for sharing information. It seemed evident that it should be a space in which anyone could be creative, to which anyone could contribute. The first browser was actually a browser/editor, which allowed one to edit any page, and save it back to the web if one had access rights.

Strangely enough, the web took off very much as a publishing medium, in which people edited offline. Bizarely, they were prepared to edit the funny angle brackets of HTML source, and didn't demand a *what you see is what you get* editor. WWW was soon full of lots of interesting stuff, but not a space for communal design, for discource through communal authorship.

Now in 2005, we have blogs and wikis, and the fact that they are so popular makes me feel I wasn't crazy to think people needed a creative space. In the mean time, I have had the luxury of having a website which I have write access, and I've used tools like Amaya and Nvu which allow direct editing of web pages. With these, I haven't felt the urge to blog with blogging tools. Effectively my blog has been the Design Issues series of technical articles.

That said, it is nice to have a machine to the administrative work of handling the navigation bars and comment buttons and so on, and it is nice to edit in a mode in which you can to limited damage to the site. So I am going to try this blog thing using blog tools. So this is for all the people who have been saying I ought to have a blog.

Thank you for the comments."

Sir Tim Berners-Lee and his blog (photomontage).

Submitted 19 December 2005: "Oops! Thanks for all the wonderful welcoming comments. We've had rather a lot, and had to turn the comments off on the first blog. I can't answer them all, but I would point out one thing. I just played my part. I built on the work of others – the Internet, invented 20 years before the web, by Vint Cerf and Bob Kahn and colleagues, for example, and hypertext, a word coined by Ted Nelson for an idea of links which was already implemented in many non-networked systems. I just put these technologies together. And then, it all took off because of this amazing community of enthusiasts, who have done such incredible things with the technology, and are still advancing it in so many ways.

By the way, this blog is at DIG, the Decentralised Information group at MIT's CSAIL. I intend it to be geeky semantic web stuff mostly. For example, it won't be for W3C questions which should be addressed to working groups.

So thanks for all the support, no need for more general 'thank you' comments! Thank *you* all."

CERN enforces Web-authoring encryption to ensure security

Web authoring is the action of editing a website's content, typically using Web-authoring applications such as Microsoft FrontPage or Macromedia Dreamweaver.

To ensure document confidentiality and to protect user passwords from possible theft, all Web-authoring actions will be required to use encryption as of 15 February.

The instructions about using FrontPage or Dreamweaver have been modified accordingly on the CERN Web Services site at http://cern.ch/web. All users are encouraged to apply the new instructions immediately.

Here are some questions and answers about this change. If you need more help, please contact the helpdesk or web.support@cern.ch.

Who does this change concern?
All persons who use FrontPage or Dreamweaver to edit a website that is hosted centrally by CERN Web Services.

Why is this change taking place?
Authoring a website requires that you supply your user name and password. If the Web-authoring application does not use a secure, i.e. encrypted, communication channel to connect to the Web server, there is a risk that your password may be stolen. By requiring an encrypted communication channel, your password is protected from theft.

How does it affect me?
From 15 February it will not be possible to author a website with FrontPage or Dreamweaver without using encryption.

Whether or not encryption is used depends on how the website is opened in your Web-authoring application. This means that you may have to change the way you open your site in Dreamweaver or FrontPage if you do not yet use encryption.

This change affects only the use of FrontPage or Dreamweaver to edit a website. There is no impact on the actual website, its functionality or its contents.

How to ensure encryption is used?

- FrontPage: start FrontPage, go to the File menu, Open site… and type the URL https://mysitename.web.cern.ch/mysitename (note the "s" in "https"), then click "Yes" if a security alert appears (figure 1).
- Dreamweaver: change your site definition to use the Local/Network connection method, with path \\mysitename.web.cern.ch\mysitename.

For more details, read the online instructions about using FrontPage or Dreamweaver to edit a website on http://cern.ch/web/docs/AuthDoc/EditWeb.

Note that both FrontPage and Dreamweaver remember how you last edited your website, so that you can re-open the website more quickly the next time. It is likely that your current shortcut or site definition is not using encryption.

As a result, you have to fully follow the instructions at least once to create new shortcuts or site definitions that use encryption, before you can use the shortcuts again.

Why do I get a security alert with FrontPage?
To encrypt communications with the Web server, FrontPage uses the HTTPS (Secure HTTP) protocol. HTTPS communications require that the Web server provides a digital certificate that proves its identity. If FrontPage cannot verify the Web server's identity, a security alert is displayed to the user.

Since HTTPS supports only one identity per Web server, the Web server always identifies itself with its actual name (e.g. webh01.cern.ch) even if a website is opened in FrontPage using the website's name (e.g. mysitename.web.cern.ch). FrontPage detects this name mismatch and shows the security alert. You can click "Yes" to proceed.

Fig. 1 (left): security alert from FrontPage. Fig. 2 (above): use the task bar to bring the hidden message box to the front.

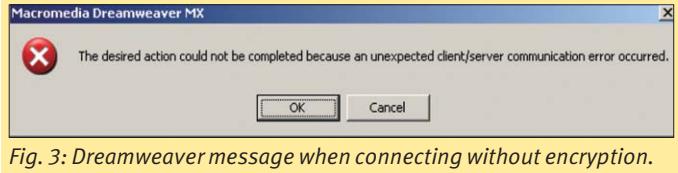


Fig. 3: Dreamweaver message when connecting without encryption.

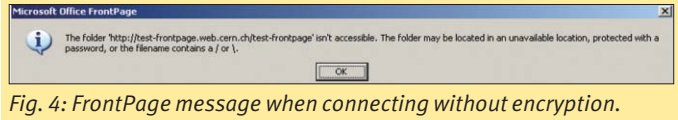


Fig. 4: FrontPage message when connecting without encryption.

How do I remove the security alert in FrontPage?
For the security alert not to appear, the website must be opened in FrontPage using the name of the actual server that is hosting your website. The server name is visible in your website's properties on http://cern.ch/web.

For instance, if the website mysitename is hosted on server webh01, use the URL https://webh01.cern.ch/mysitename (instead of https://mysitename.web.cern.ch/mysitename) in FrontPage. This will match the name on the digital certificate that proves the server identity, and the alert will not reappear.

Note that the actual server name for your website can change from time to time. Please refer to your website's properties for the latest information.

FrontPage seems to freeze when I open my website.
Sometimes FrontPage may appear to freeze when you try to open a website. It is actually waiting for you to click on the security alert message box that is hidden by the main FrontPage window (figure 2).

The solution is to use the task bar to bring the hidden message box to the front.

What will happen if I try to connect without using encryption?
After 15 February, if you do not use encryption your Web-authoring software will report that it cannot find your website.

What should I do if Dreamweaver shows the following error message: "The desired action could not be completed because an unexpected client/server communication error occurred" (figure 3)?
You are probably trying to connect without encryption. Follow the instructions from http://cern.ch/web/docs/AuthDoc/EditWeb to open your website using encryption.

What should I do if FrontPage shows the following message: "The folder 'http://test-frontpage.web.cern.ch/test-frontpage' isn't accessible. The folder may be located in an unavailable location, protected with a password, or the filename contains a / or \" (figure 4)?
See answer to previous question.

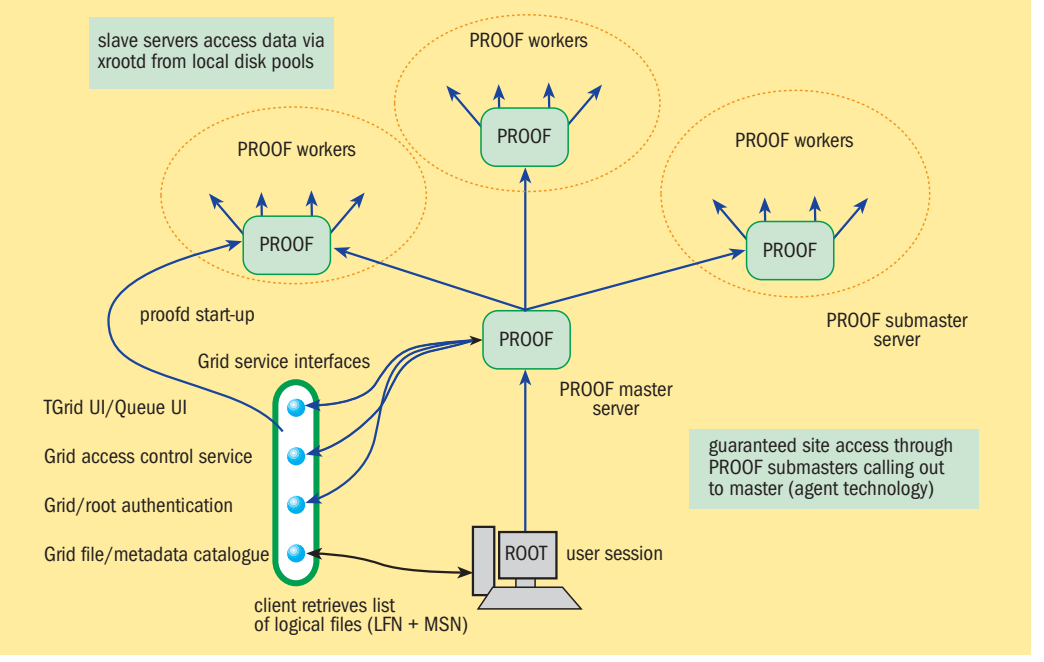
I cannot open my site in FrontPage from Internet Explorer.
The Edit with Microsoft Office button in Internet Explorer will not work anymore, because this feature does not use encryption.

Alexandre Lossent, IT/IS

PROOF will analyse LHC data

The Large Hadron Collider (LHC) experiments will generate huge amounts of data, and special methods will be needed to analyse them efficiently. No single computer will be able to crunch the data in a reasonable amount of time.

The only way to cut analysis time to an acceptable level is to use parallelism. Depending on the amount of data, parallelism can be employed on multicore laptops, local clusters or global distributed clusters, i.e. the Grid. The challenge will be to provide this parallelism transparently so that users won't have to worry about how to access all of these resources in parallel.



Multi-tier PROOF architecture with the client talking to a master, the master talking to the submasters, and each submaster talking to a group of worker nodes. In a Grid environment the location of the submasters and workers will be determined by the location of the data files that are to be analysed.

The ROOT framework

From the mid-1990s, the ROOT system was developed to offer the functionality needed to handle and analyse large amounts of data. ROOT, which is an object-oriented framework, offers an extensive set of tools for data storage, analysis and presentation. The data are defined as objects, and special storage methods are used to get direct access to the separate attributes of the selected objects, without having to touch the bulk of the data. The system was designed to query its databases in parallel on parallel-processing machines or on computer clusters.

ROOT is the preferred data analysis environment for the LHC experiments, so the ROOT team has increased its efforts to provide a system that will give efficient access to many computers in parallel.

PROOF provides transparency

The Parallel ROOT Facility (PROOF) enables distributed data sets to be analysed interactively in a transparent way. It exploits the inherent parallelism in data from uncorrelated events via a multi-tier architecture that optimizes I/O and CPU use in heterogeneous clusters with distributed storage. Being part of the ROOT framework, PROOF inherits the benefits of a performant object-oriented storage system, and statistical and visualization tools.

PROOF requires the analysis to be run via "selectors" that contain user code that is called by the PROOF worker nodes. PROOF opens the ROOT files that are to be analysed and tries to optimize the data-access patterns so that workers read data locally or via the high-performance xrootd file servers. Since many PROOF selectors typically are I/O bound, the efficiency of the data-access infrastructure largely determines the efficiency of the system.

Selectors are a universal way of processing ROOT files and can be run transparently in a local ROOT session or on a PROOF cluster. Selectors can be interpreted with CINT or compiled on the fly with the ACLiC mechanism (ROOT's transparent C++ compiler interface). The user code in the selectors can access experiment or user shared libraries, which can then be uploaded, compiled and installed with the PROOF package manager. This mechanism enables PROOF cluster nodes to have a different architecture, operating system or compiler from the platform on which the user developed the code.

Suitable for long-running jobs

Initially PROOF was developed purely for interactive analysis, with queries lasting no more than several tens of minutes and operating in synchronous mode – i.e. the lifetime of a PROOF session was determined by that of the client session. We have recently extended PROOF to support the "interactive batch" mode, in which a user can close the local client session while the PROOF query continues to run on the remote cluster. The user can later reconnect to the PROOF cluster to inspect progress or get the results of finished queries.

The advantage of using PROOF for long-running jobs (instead of splitting the analysis into multiple-batch jobs, each running over part of a data set) is that the selector and analysis model does not change depending on the length of the query or the size of the data set. This means that a more dynamic and interactive monitoring of the intermediate results is possible.

PROOF can also be distributed over several sites if data sets span more than one site. In this case, PROOF has to operate with the Grid file and metadata catalogues, and authentication and job-submission systems.

Typically, a user will query the file catalogues for a data set to be analysed. The location of the files in the data set determines where PROOF worker nodes have to be started by the Grid job-submissions system. Once the PROOF worker agents are started, the user's client session will connect to the master and the queries can be executed (see figure). A prototype of this model, which combines AliEn (the ALICE file catalogue and job-submission system) with PROOF, was demonstrated at the 2005 Supercomputing conference.

This year the ROOT team will improve PROOF and help the LHC experiments to integrate it into their analysis and Grid environments.

Further information

- ROOT – http://root.cern.ch;
- xrootd – http://xrootd.slac.stanford.edu;
- CINT – http://root.cern.ch/root/Cint.html;
- AliEn – http://alien.cern.ch.

Fons Rademakers, PH/SFT, CERN

Grid technology helps UNOSAT to tackle humanitarian challenges

Patricia Mendez Lorenzo is part of the LCG Experiment and Integration Support Team at CERN. Normally she supports ALICE, helping LCG sites to install and run the ALICE software. But last summer she was assigned an additional task: to help gridify satellite imagery applications for UNOSAT, a United Nations initiative that provides the humanitarian community with access to satellite imagery for use in crises such as earthquakes and tsunamis.

CERN has hosted the UNOSAT team for the past four years, so that it can benefit from CERN's substantial IT infrastructure and Internet access. Tapping into CERN's Grid know-how was another reason, and last year a summer student project, supervised by Mendez Lorenzo and Einar Bjorgo of UNOSAT, provided an ideal opportunity to push forward on this front.

CERN's Patricia Mendez Lorenzo and UNOSAT's Einar Bjorgo have adapted satellite imagery tools to the Grid.

With Sean Moran, a student from Cambridge University, they began by transferring some 3.5 TB of data on the Asian tsunami to the CASTOR storage management system. They then set up a software infrastructure to enable the UNOSAT team to access the data using standard LCG tools. At the same time, Mendez Lorenzo and Bjorgo created a virtual organization for UNOSAT, with a view to extending this to other sites around the globe that UNOSAT collaborates with. In this way, in future this sort of data can be stored in a truly distributed way.

With members of the ARDA project, led by Massimo Lamanna, Bjorgo and Mendez Lorenzo implemented metadata applications that enable stored data to be searched according to geographical co-ordinates. They also interfaced computer-intensive UNOSAT programs to LCG. These programs can heavily compress satellite images for transmission over low-bandwidth connections to relief workers in the field. Mendez Lorenzo has continued to test these Grid applications and was invited to present the results at a workshop during the 1st IEEE International Conference on e-Science and Grid Computing in Melbourne, Australia, in December.

"Gridifying an application like this from zero is gratifying," said Mendez Lorenzo, "because you get to develop the whole infrastructure and see applications run in a relatively short time." The UNOSAT team is equally enthusiastic, and is already planning the next stage of this development project – to adapt more of the UNOSAT software suite to the Grid – with Mendez Lorenzo and LCG.

François Grey, IT/DI, CERN

Canada's TRIUMF is home to ATLAS Tier-1 centre

TRIUMF, Canada's national laboratory for particle and nuclear physics, will host a Tier-1 centre for the ATLAS experiment. By 2008 the centre will include 1900 kSI2k of CPU power, 1000 TB of disk storage and 730 TB of tape storage. Funding has been requested from the Canada Foundation for Innovation. A review is scheduled to be held in January 2006, and a decision is expected by February.

Canada's current involvement in the LCG includes developing and deploying middleware for the Grid. In particular, TRIUMF, which is located in Vancouver, is hosting several LCG site/cluster solutions. These include:

- a modest, fully fledged local LCG cluster;
- a gateway that unites resources at Canadian universities and makes them accessible to LCG as one site, via a computing element that uses CondorG technology (this is a unique Canadian initiative, see www.gridX1.ca);
- a development cluster that is dedicated to the service challenges on which LCG baseline services are deployed and tested. The main focus at TRIUMF last year was to set up the components to participate in all aspects of LCG Service Challenge 3, such as disk-to-disk and disk-to-tape transfers between CERN and TRIUMF, and disk-to-disk transfers between TRIUMF and several Canadian universities that were acting as Tier-2 centres;
- a distinct LCG executor based on CondorG (and hosted by TRIUMF and Simon Fraser University), which has doubled ATLAS's overall capacity for production and job submission on the Grid. This was crucial to complete the Monte Carlo samples that were needed for last year's ATLAS Physics Workshop, held in Rome.

The networking resources are provided by CANARIE, and at the moment comprise 2×1 Gbit/s dedicated lightpaths that were made available in spring 2005 and used in Service Challenge 3 last summer. A 10 Gbit/s line is now being commissioned and should be available in the first quarter of 2006.

In June 2005 a temporary 10 Gbit/s lightpath between CERN and TRIUMF was available for several days. This lightpath was used for various transfer tests. A sustained transfer rate of 2.33 Gbit/s was achieved.

R Tafirout, TRIUMF; M C Vetterli, Simon Fraser University/TRIUMF

A 'defence-in-depth' strategy to protect CERN's control systems

Ten years ago control systems were restricted to dedicated processes that had sparse interconnectivity with other systems, if at all. The hardware was based on proprietary technologies, and communication protocols were custom designed or came from only one or a few vendors. As such, the control systems were completely (or mostly) separated from the rest of the world and only reachable by means of a few dial-up modems.

From the point of view of security these systems were safe ("security through obscurity"), since only a few experts had knowledge of the protocols and methods used, and outside connectivity was low. Major threats were insiders (e.g. disgruntled employees) who might target the control system for personal gain, or users who badly configured the system. However, a recent analysis reports that today the dominance of internal fraud is rapidly being replaced by threats created externally [1].

During the 1990s, in parallel to control systems, standards based on Ethernet and the TCP/IP protocol were introduced into information technology (IT) networks. Because of their openness and ease of use, these networks spread around the world and became the standard for office and business networks as well as for use at home.

However, with this openness, and because no software or operating system is free of flaws, there was a downside in the form of "war dialling", "backdoors", password sniffing and cracking, and the hijacking of user sessions.

These threats, which started in the mid-1990s, became more sophisticated. As hackers accumulated knowledge, new viruses and worms automated the attacks. Today IT is faced with Internet Relay Chat (IRC)-based intrusions, denial-of-service attacks, botnets and zombie machines, which can strike with a synchronized attack from hundreds of machines around the world.

ICALEPCS 2005, where the CNIC working group presented its policy document on protecting CERN's control systems from cyber-attacks.

Control systems join IT networks

Many control systems are now undergoing a change towards modern IT-based solutions, with common IT standards being applied to control systems and networks. Proprietary field buses are being replaced by Ethernet and TCP/IP. Common IT protocols such as SNMP, SMTP, FTP, Telnet and HTTP are being used to share data from control systems with data warehouses, the upper management levels ("from top floor to shop floor") and the outside world. More and more sensors, actuators and other field devices are being connected to this network.

Furthermore, commercial off-the-shelf (COTS) IT hardware now enables virtual private network (VPN) access from remote locations (e.g. from home) to the controls network, and permits wireless communication with it.

On the user interface side, operator consoles and Supervisory Control And Data Acquisition (SCADA) systems are now based on the Microsoft Windows platform or are ported to a standard Linux installation. Notebooks and USB sticks have become new means to monitor and configure control systems.

Controls are open to attack

However, the rise of modern IT in control systems and networks also has drawbacks. The close interconnectivity between controls and office networks enables viruses and worms to spread more easily to control systems. Remote VPN or wireless access, notebooks and USB sticks offer new possibilities for a virus or worms to enter the controls network. Not to mention hackers and terrorists who might be interested in targeting controls computers to shutdown the system.

Since Microsoft's Windows operating system is now the *de facto* platform for SCADA applications, the corresponding control PCs inherit the same vulnerabilities that office PCs have. Linux-based controls PCs do too. Unfortunately controls PCs cannot be patched and updated as fast as office PCs, and some might even lack antivirus software because of interference with the control processes. Even if these PCs are secured, zero-day exploits might enter before the proper patch or virus signature file is available or applied.

Users and operators of control systems are the next weak link. First they might carry infected notebooks into the control room or connect their infected home PC to the controls network via VPN. Second, in the era of legacy control systems passwords were known to many people and still are. These passwords might also be weak, in the sense that they consist of a few letters only or can be found in a dictionary. For convenience, passwords might even be written on a sticker and fixed directly onto a terminal. In addition, many applications still use the default password or may have no password at all. In the past, traceability was guaranteed owing to the restricted group of people that had access to the control system, but with the new interconnectivity, password sniffing can be done remotely and automatically.

Last but not least, COTS automation systems such as programmable logic controllers (PLCs), power supplies and other field devices generally have no security integrated into their designs. Of a range of such devices tested at CERN with a standard IT security scanner for vulnerabilities, more than 30% failed to communicate properly [2]. Even worse, manufacturers are including more and more IT functionality (like e-mailing and Web servers) into these devices, which is reducing security even further.

CNIC presents mitigation strategy

More than 110 different control systems are now operational or under development at CERN. These systems monitor, control, supervise and safeguard CERN's accelerators, experiments and infrastructure – from buildings, electricity and heating to access control, radiation protection and safety. Many systems use today's standard technologies mentioned above. The corresponding PLCs, VME crates and PCs that run Linux, LynxOS or Windows operating systems are connected to CERN's local-area network (LAN) using the TCP/IP protocol in one way or another. However, apart from the range of IP numbers, no clear distinction has been made

between office and controls applications, neither for networking nor configuration.

To refine the use of control systems at CERN and to offer methods to protect them, the working group called Computing and Network Infrastructure for Controls (CNIC, see http://wg-cnic.web.cern.ch/wg-cnic) has produced a security policy document [3]. This document was presented at the International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS05) in Geneva, Switzerland, last October. The document follows closely the best-practice standards that are used increasingly in industry, and, to achieve an acceptable level of protection, follows a "defence-in-depth" approach. Here is an outline of its recommendations:

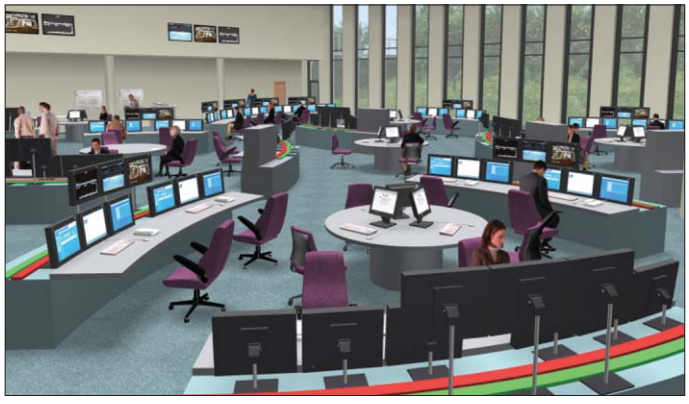
● Separation of the controls networks (i.e. dedicated networks for accelerators and experiments) from the office network, and additional segregation of the controls networks.

The CERN LAN now consists of two different physical networks: the General Purpose Network (GPN) and the Technical Network (TN). The former is used for all office (campus) computing and for development, while the latter is used to run the control systems for all accelerators (AB and AT departments), for safety precautions (the safety commission), and for site-wide monitoring (the TS department). They were fully separated, in terms of interconnectivity, on 9 January.

Four additional networks are planned or have been installed for the LHC experiments ALICE, ATLAS, CMS and LHCb. More dedicated controls networks might be envisaged for fixed-target experiments. Inside each network, further access restrictions, such as local firewalls and network filtering, will enable the protection of sensitive equipment.

● Channelled paths to access controls networks remotely, and rules for handling notebooks, wireless and VPN connections – to protect these controls networks from outside threats.

Access to each of these controls networks is restricted. Direct data exchange is inhibited except for a few "trusted" central IT services such as DNS, NTP, AFS, DFS and Oracle DB. However, users are guaranteed access through Linux and Windows-based application gateways, which require proper authorization. The use of wireless access, VPN access and notebooks on a controls network are generally prohibited. Wireless and VPN accesses are still possible from the GPN through the corresponding application gateway.



A computer simulation of the control centre for CERN's Large Hadron Collider. The centre is expected to be operational by 1 February.

● Procedures to register devices being connected to a controls network, to manage control systems under the responsibility of the users, and to intervene in the case of a security incident.

For each controls network, one or more domain managers have been appointed to implement and follow up the CNIC security policies and adapt them where necessary. The managers authorize devices that need to be connected to a controls network. For this, each device must be properly registered in the network database that is managed by IT/CS (http://networking.cern.ch). The domain managers also follow up security incidents with CERN's Computer Emergency Response Team (CERT).

● Methods to secure controls PCs and to centrally manage the installation, patching and upgrading of their operating systems and application software under the responsibility of the control system experts.

The existing installation, patching and upgrading procedures for Windows and Linux PCs are inappropriate for controls PCs, since they leave little control to the user in terms of what to install and when to reboot the PC. To mitigate this, the IT/FIO and IT/IS groups have developed new tools named Linux for Controls (LinuxFC) and Nice for Controls (NiceFC).

Each user can create one or more sets of PCs and take over the responsibility of these. For each set, the user can define precisely which centrally managed operating system and which application software should or might be installed, and for which applications installation is denied. The users keep full control of when these applications are applied and when to reboot the PCs.

Furthermore, no automatic patching or upgrading will be carried out. Instead, the manager of a targeted system will receive e-mail notification to apply the patches as soon as possible. However, although patching is not automatic, failure to apply a patch within a defined time limit may lead to a PC being disconnected from the network if it poses a risk to the overall integrity.

● Rules on user accounts and passwords to enforce traceability.

Users are often the weakest link in the security chain, especially owing to their choice of weak passwords. Furthermore, generic accounts (e.g. operator accounts) that are used to operate control systems are not bound to one person, and the corresponding passwords are frequently known to many people. The CNIC policy requires users to employ strong passwords. It also imposes a verification of all generic accounts and their removal where possible. In any case, traceability must be guaranteed in every case, e.g. through physical access protection.

● Raise awareness of security issues in the users community.

Security starts with users, so CNIC has launched an awareness campaign to inform all users of control systems of the possible risks and threats. CNIC also organizes weekly users exchange meetings, where problems are discussed and solutions presented. Finally, the CNIC TWiki (https://uimon.cern.ch/twiki/bin/viewauth/CNIC/WebHome) documents all CNIC-related issues and offers a platform to discuss problems further. Every user of control systems at CERN is encouraged to join one of these activities.

Conclusion

With the adoption of modern IT standards by control systems, and the subsequent growing interconnectivity between campus networks and control networks, control systems have become exposed to the same weaknesses that threaten computer security. However, most control systems are not able to defend themselves against such cyber threats.

Therefore, the CNIC working group has produced a security policy document that proposes various means of mitigating an attack. In particular, all control systems at CERN must be properly secured by a "defence-in-depth" strategy. Users of control systems are invited to participate in this discussion. The threat is real, and so the primary question must be "Do we act before or after an incident?"

References

[1] E Byers, Who Turned Out the Lights? Understanding the Changing Risks to Critical Control Systems from Cyber Attacks to Viruses – New Trends in Threats and Implications, ISA EXPO 2004.
[2] S Lüders, Control Systems Under Attack?, ICALEPCS05.
[3] U Epting *et al.*, Computing and Network Infrastructure for Controls CNIC, ICALEPCS05.

Stefan Lüders, IT/CO

US HEPiX attracts large audience

Participants at the autumn meeting enjoyed talks on collaboration tools, CPU benchmarks, Linux, and disk and storage systems among others.

The autumn 2005 HEPiX meeting was held at the Stanford Linear Accelerator Center (SLAC) on 10–14 October. Confirming the trend from last year, the US meetings now attract as large an audience as European meetings – more than 80 this time from some 27 institutes in Europe and North America.

The meeting, which was impeccably organized by Chuck Boeheim and colleagues, comprised a day of sessions on collaboration tools, followed by three days of "normal" HEPiX sessions, and finally a half day of talks on hardware issues.

Collaboration tools day

The first day was a review of some common collaborative tools, highlighting possible trends in videoconferencing in particular. The talks included some from non-typical HEPiX speakers who had stopped at SLAC on their way to an ESnet conference in Berkeley.

The afternoon session was largely drawn from information gathered by RTAG12, a requirement technical assessment group of the LHC Computing Grid project. The session included a summary of a report by the RTAG12 chairman, who closed his talk with personal suggestions on how to move forward on the report's recommendations. There was also a talk on how to select the most appropriate electronic document management system tool for the International Linear Collider study.

The following collaborative tools were presented: Wiki (at GSI, Darmstadt, and at FZK, Karlruhe); the Form Factory tool being built at DESY; the Indico tool developed at CERN; the Skype peer-to-peer telephony system over IP; the Access Grid high-performance video conferences, which are widely used in the UK; the collaborative tools in NICE at CERN (such as WebDAV access to DFS, and Windows Terminal Services); the Virtual Room Videoconferencing System; VACS, the home-written management system that is used in France; and the Web-hosting services at CERN.

HEPiX session highlights

The following are a selection of other highlights from the meeting. Please note that not all sessions are covered, and points are in no particular order. More details can be found on the SLAC website(www.slac.stanford.edu/conf/hepix05/agenda.html).

- Collaboration was evident throughout the week, with many system and sysadmin tools appearing in laboratories across the HEP community; for example, Scientific Linux, Quattor, dCache and Xrootd. At HEPiX came the first indication that CERN's monitoring tool, Lemon, may be the latest package to be of more general interest.

- As at the last meeting, most sites reporting CPU farm increases are buying Opteron systems – BNL and CERN being exceptions. In this area, an interesting set of benchmarks performed at GridKA on different processors was reported on the final day (see SLAC website).

- At a batch workshop follow-up, Tim Bell presented some changes made following input at the last HEPiX meeting. Francesco Prelz, the main Enabling Grids for E-sciencE (EGEE) batch system developer, then presented his open questions, which resulted in a productive exchange and a plan to move forward on a topic that has been unresolved for some time. It was agreed to follow this up at the next meeting. Francesco said he felt the session had been valuable, and that HEPiX had provided a welcome forum to make this happen. The HEPiX board has agreed to make this happen in CASPUR and perhaps in future meetings as needed.

- Regarding Linux, Fermilab proposed that we consider making HEP code comply with Linux Standards Base. There was a discussion about differences and compatibility between Scientific Linux (SL) and Scientific Linux CERN (SLC). Some concern was expressed that CERN, unlike other labs, had issued its tailored version of SL as a formal SLC release. It apparently confuses some users, at least those outside CERN, who are associated with LHC experiments. CERN either needs to reconsider this branding or to advertise better what it is, why we do it, and the fact that it is, or should be, binary-compatible with the SL from Fermilab.

- An interesting set of sessions was held on disk and storage systems, including DPM, SRB, Xrootd, dCache and Panasas.

Comments

All CERN talks from the Internet Services groups included a live demo. While this is not always possible (Hege Hansbakk thought of doing one for Licence Monitoring, but off-site access to the pages is forbidden), it should be considered where possible.

The organizers made a deliberate effort to schedule several talks that were targeted at the physics that is happening or is planned to take place at SLAC, rather than at our usual range of only computing subjects. These additional talks (given by the director, Richard Mount, and by an astrophysics theorist) were quite interesting, and the last one in particular was entertaining.

Trip report

For those who are interested, a more detailed report about the HEPiX meeting is stored in Indico. Also, the SLAC HEPiX Report (summary and slides) that was presented at the joint Computing/After-C5 seminar in October 2005 is available at http://indico.cern.ch/conferenceDisplay.py?confId=a056269.

Future HEPiX meetings

The next meeting will be at CASPUR in Rome, Italy, on 3–7 April. The autumn meeting will be held at the Jefferson Lab.

Alan Silverman, IT/DI

Users must be suspicious when reading e-mails

Techniques used by spammers evolve continuously and are becoming very clever. Last December CERN was attacked by a malicious e-mail in which the user was invited to access a URL. By selecting the URL some users have infected their PCs with a virus. Unfortunately there is no reliable way to distinguish a fake e-mail from a real one. Below we provide some guidelines to help you recognize whether an e-mail should be considered suspicious.

What should I check?
Read the text carefully.
- Does it contain account-specific data (such as the real [first] name or physical location of a network device)?

While most of these data can probably be gained from some publicly visible information, it is much easier for a legitimate mail sender (with direct access to CERN's internal databases) to obtain such information. As you can see in the example, the message was not precise, referring to "your account" (without any indication to which machine and login it was referring to at CERN), and "for security reasons" (without giving any further explanation).

- Look for small errors in titles or names.

In the example, the signature is given as "Cern Security Department", which does not exist (it is the CERN Computer Security team).

These indicators should be enough to make you suspicious about an e-mail already.

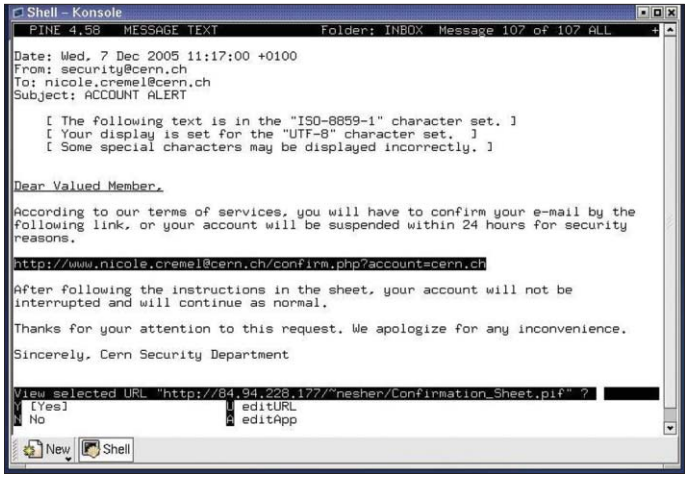
Suspicious URL
A good way to check if a URL is what it claims to be is to type it (do not cut and paste it) into your browser. However, most mail clients have features that are easier to use.
- If you read your mail (HTML format) on NICE using Outlook, or on Linux using GNOME Evolution, pause the cursor over the highlighted URL. Check if the real URL that appears in a yellow box (in Outlook) or in a status bar at the bottom of the screen (Evolution) looks trustworthy. In the example, the URL pointed to a strange address outside CERN.
- If you use pine and hit return next to the URL, the real URL will appear at the bottom of the screen along with a request to confirm that you really want to go there.

Suspicious attachment
If the suspicious mail comes with an attachment, another good indicator is whether the right "tool" (file format) is being used for the message:
- A short notification is best handled by plain text.
- A complex, multipage document will probably arrive as a .doc or .pdf attachment.
- Unless you are expecting a collection of binary files that only make sense together (so adding them as individual attachments won't work), a .zip file is highly suspicious.

On Windows, it is strongly recommended to save attachments before viewing them, because a virus scan is automatically performed when saving the file. This is true even for attachments that come from someone you trust, as their computer may be infected.

Fighting this problem
The IT department is investigating further techniques to combat spamming. There are ways to fight these bogus e-mails but this means imposing stricter rules, which will eventually lead to less convenience for users; the challenge is to find the right balance. Meanwhile we have to rely to some degree on users being proactive and suspicious. As was written in the last issue of *CNL*, in case of doubt users should ask the helpdesk before taking any action.

Nicole Crémel, IT/UDS;
Judy Richards, IT/DI



From: security@cern.ch
To: Nicole Cremel
Subject: ACCOUNT ALERT

Dear Valued Member,

According to our terms of services, you will have to confirm your e-mail by the following link, or your account will be suspended within 24 hours for security reasons.

http://www.nicole.cremel@cern.ch/confirm.php?account=cern.ch

After following the instructions in the sheet, your account will not be interrupted and will continue as normal.

Thanks for your attention to this request. We apologize for any inconvenience.

Sincerely, Cern Security Department

An example of a malicious e-mail sent to CERN last December.

The deadline for submissions to the next issue of CNL is

3 March

E-mail your contributions to cnl.editor@cern.ch

If you would like to be informed by e-mail when a new issue of CNL is available, subscribe to the mailing list cern-cnl-info. You can do this from the CERN CNL website at http://cern.ch/cnl

IT database staff gain Oracle 10g certification

Oracle database administrators recently attended two training courses on the latest 10gR2 release of the software. The courses were offered following co-operation between the groups HR/PMD (Human Resources Personnel Management and Development) and IT/DES (Database and Engineering Services).

The main motivation behind the courses was to offer experts in database administration high-quality training that would match their demanding job. Another asset was to give participants the opportunity to get certified in Oracle 10g and thus to receive recognition for their skills, even outside the organization.

The first course was held on 2–4 November and was designed for people who passed the Oracle 9i certification last year. Eleven people attended: five from IT/DES, four from IT/ADC (Architecture and Data Challenges), and two from IT/AIS (Administrative Information Services).

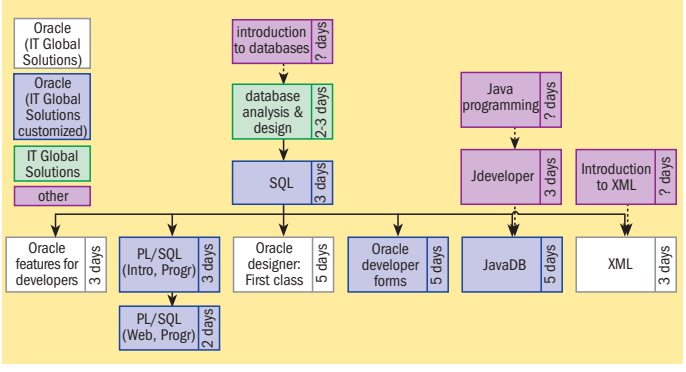
The second course, which took place on 7–11 November, was designed for people who did not have the Oracle 9i certification. Seventeen people attended it: three from IT/DES, four from IT/ADC, three from IT/AIS, four from IT/FIO (Fabric Infrastructure and Operations), two from IT/CS (Communication Systems), and one from TS/CSE (Technical Support Department, group "Controls, Safety and Engineering Databases").

Both courses were held at the Oracle Training Office, at the World Trade Centre, Geneva.

The attendees thanked the organizers who made this event happen. These Oracle 10g courses will undoubtedly help the newly certified database administrators to continue to address the evolving needs of the database users' community and to improve the overall quality of the many CERN services that are based on Oracle.

CERN Technical Training services provides a complete curriculum on Oracle, called the Oracle Training Curriculum @ CERN. You will find information about dates and registration on the CERN Technical Training website at http://cern.ch/HR-web/external/training/tech/software/te_softw.asp.

Catherine Delamare and Montse Collados, IT/DES



The organization of the Oracle Training Curriculum @ CERN.

Recent changes to IT services

Changes to services in the IT department are published on the Service Status Board (SSB), which is located at http://cern.ch/it-servicestatus. The most recent changes and their dates of posting are shown below. The SSB also includes power cuts, scheduled interventions, service incidents, and the status of most services. A dynamic page with the status of most services is also available at http://cern.ch/itservicestatus/dynamic/.

18 November 2005	Oracle Forms 6i migration to Forms 10g (summer 2006)
19 December	Restrictions on the CERN VPN service
15 December	e-MAPS form is available in EDH
12 December	EDH – new options: "Confidential" and "Urgent" in the DAI document
25 November	New tutorials for EDH
25 November	New profile for user accounts in DEVDB
21 November	AIS-NICE login synchronization
21 November	Change in EDH Material Request form
17 October	NICE login is mandatory for all operations via the network Web interface
14 October	TCP and UDP port 3372 blocked in firewall

The CNL team wishes you a happy New Year for 2006!

Calendar

February
13–16 **16th Global Grid Forum (GGF16)**
Athens, Greece
www.ggf.org/GGF16/ggf_events_ggf16.htm

13–17 **15th International Conference on Computing in High Energy and Nuclear Physics (CHEP06)**
Mumbai, India
www.tifr.res.in/chep06

March
1–3 **EGEE User Forum**
Geneva, Switzerland
http://egee-intranet.web.cern.ch/egee-intranet/User-Forum/index.html

1–3 **TridentCom 2006**
Barcelona, Spain
www.tridentcom.org

April
2–6 **High Performance Computing Symposium (HPC 2006)**
Huntsville, Alabama
www.caip.rutgers.edu/hpc2006

3–7 **HEPiX meeting**
Rome, Italy
www.hepix.org

25–29 **20th IEEE International Parallel and Distributed Processing Symposium**
Rhodes Island, Greece
www.ipdps.org

June
27–30 **ISC2006**
Dresden, Germany
www.supercomp.de
Paper deadline 20 February

August
29–1 September **Euro-Par 2006**
Dresden, Germany
www.europar2006.de
Paper deadline 31 January

September
13–15 **HPCC-06**
Munich, Germany
http://hpcc06.lrr.in.tum.de
Paper deadline 13 March

October
25–27 **eChallenges 2006**
Barcelona, Spain
www.echallenges.org
Paper deadline 28 February