ISSN 1356-0735

DATAWATCH

VOL. 44 MAR-MAY 2000

IN THIS ISSUE:

PKI

ORACLE -

E-COMMERCE

THE QUARTERLY MAGAZINE OF ISACA LONDON CHAPTER

VOLUME 44 MAR-MAY 2000

DATAWATCH

is a quarterly magazine
published by the

Information Systems Audit and Control Association

London Chapter

Chapter Office:
10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE17 1SD

In this issue:

FEATURES

REGULARS

PLUS

ISACA London Chapter Committee 1999/2000

PRESIDENT
John Mitchell
LHS Business Consultancy
01707 851454
Lhs@lhscontrol.co.uk

VICE PRESIDENT
Steve Bailey
Steve Bailey Associates
01480 432602
Spart@compuserve.com

TREASURER
Archie Watt
BDO Stoy Hayward
0171 893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Charles Mansour
The Woolwich
0181 298 5646
Charles.Mansour@woolwich.co.uk

MEMBERSHIP
Kamal Khan
Sanwa Bank Ltd
0171 330 5522
kamal.khan@sanwabank.co.uk

PUBLICATIONS
Annabel Lane
Nestle UK Ltd
0181 667 6530
annabel.lane@nestlegb.nestle.com

SIGS
John Hunter
HLB International
01635 248944
mailbox@jhunter.u-net.com

SIGS
Bill Hawkins
Corporation of London
0207 332 1296
Bill.Hawkins@corpoflondon.gov.uk

MARKETING
Derek Oliver
Ravenswood Consultants
01268 794556
consultants@ravenswood.co.uk

EVENTS
Karen Sharpe
Deloitte & Touche

karen.sharpe@deloitte.co.uk

CISA CO-ORDINATOR
David Spaven
KPMG
0171 311 5620
David.Spaven@kpmg.co.uk

PAST PRESIDENT
Gerry Penfold
KPMG
0171 311 8489
Gerry.Penfold@kpmg.co.uk

WEBMASTER
Allan Boardman
Internet Working 4U
01732 462 133
allan@internetworking4u.co.uk

CHAPTER OFFICE
Nancy Watt
10 Drayhorse Road, Ramsey, Huntingdon, Cambs, PE17 1SD
Tel/Fax: 01487 815705

WEBSITE:
WWW.ISACA.ORG.UK/LONDON
Email:
nancy@isaca.org.uk

ISACA Northern UK Committee (officers only)

PRESIDENT
Ray Butler
HM Customs & Excise
0161 827 0875
rbutler.c&e.cau@gtnet.gov.uk

VICE PRESIDENT
Robert Newbould
British Steel
01709 825479
bob_newbould@technology.britishsteel.co.uk

TREASURER
Gillian Peschke
Pricewaterhouse Coopers
0113 289 4273
gillian.peschke@uk.pwcglobal.com

MEMBERSHIP
Lynn Lawton
KPMG
0161 838 4000
Lynn.Lawton@kpmg.co.uk

CISA CO-ORDINATOR
Alan Rainford
Axa Insurance
01253 662782
alan_rainford@gre-group.e-mail.com

WEB MASTER
Peter McCready
MBNA International Bank
01244 672000
macriada@btinternet.com

ACADEMIC RELATIONS
Mike O'Hara
University of Salford
0161 295 5665
m.j.ohara@iti.salford.ac.uk

WEBSITE:

WWW.ISACA.ORG.UK/NORTHERN

ISACA Central UK Committee (officers only)

PRESIDENT
Mike Hughes
KPMG
0121 232 3207

VICE PRESIDENT/CISA
Simon Parker
Canada Life
01707 422064

SECRETARY
Steven Babb
KPMG
0121 232 3213

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:

WWW.ISACA.ORG.UK/CENTRAL

The Editor's Chair

By Annabel Lane

Welcome to another issue of Datawatch, your award winning magazine! As indicated on the front of this issue, Datawatch has scooped the ISACA award for best newsletter for large chapters - and not for the first time, either. I realise that a tearful acceptance speech is customary at such occasions but regretfully my scene stealing opportunities may well be curtailed as no doubt the President will accept it on behalf of the Chapter. But if he gets an opportunity to cry I would like him to thank the editorial team, particularly Nancy Watt, who does the really hard work of putting the issue together from the material collected.

But that is no reflection on the standard of articles we publish and this issue is no exception. As well as the regular features we have some specialist articles revolving around this season's theme of the extended enterprise. PKI is something that's been very much in the news recently as an area that's going to affect all of us who use e-commerce - and that's going to be nearly all of us if what the industry pundits say is to be believed. Those of you wanting a comprehensive view of this subject will find Paul Healy's article on Securing E-business very interesting, as it deals with the issues behind PKI as well as explaining how it works and addressing the concept of digital signatures.

The security of Oracle databases is an area of increasing importance as more companies use this type of relational database, particularly in support of ERP systems. Karen Nelson's article talks about this in the context of the extended enterprise and goes into securing this type of database in considerable detail and relates it to the wider business context.

And now's the time of year when an IS Auditor's fancy turns to….CISA. Any CISA candidates who have been questioning their own wisdom in subjecting themselves to the torment of the lengthy CISA exam (is it just me or are some of the questions they set totally impossible?) should read Adrian Simpson from Barclay Simpson's article on the importance of qualifications. And further on this theme, Derek Oliver's article on CISA and the role of the certification board in determining its direction gives an insight into the process of setting questions and a sneak preview of possible future strategies. As ever, the opinion of you as ISACA members counts whether at global or chapter level, so if you do receive a copy of the questionnaire he mentions in the article, do use it to feedback to have your say and keep CISA a relevant and cutting edge qualification!

Email any letters to Derek Oliver at consultants@ravenswood.co.uk

Mind Games
by Puzz

The answer to each clue is a word which links with each of the three words listed. This word may come at the beginning (e.g. ODD linked with BALL, FELLOW and SOCKS), at the end (e.g VILLA linked with ROMAN, ASTON and HOLIDAY), or a mixture of the two (e.g. AGE linked with BOND, BRONZE and GAP).

Once you have solved all the clues, take the first letter of each word and rearrange them to form a word well-known to us all. Answers on page 28.

1. EYE	MARK	FRONT	.....	5. WORK	DRAG	HAIR	.....		
2. TESTING	END	FRIENDLY	.....	6. GROWTH	STAND	FLO	.....	9. BROWN	ION	DESERT	.....
3. TAR	LOST	BUD	.....	7. APACE	ROT	PET	.....	10 PLANETS	CIRCLE	SPACE	.....
4. HAT	TIMER	OLD	.....	8. THOU	PIPER	IRON	.....	11. HALF	CHAFF	MEAL	.....

From the President

By John Mitchell

Every time that we receive a request from a member that we are unable to resolve, your Management Board goes into a virtual huddle (usually via email) to see whether we can enhance the service in some cost effective way to prevent the problem reoccurring. We currently have two of these on our agenda: under capacity of space for our monthly meetings and a request to be able to preview publications from International's book store prior to purchase. I have dealt with the first issue in the last two editions of the Mailshot, so I will not repeat here what I have already told you, but I will reemphasise that we are desperately trying to resolve that particular problem. The matter of previewing publications however, has only recently arisen and is still being debated. The basic problem is that no-one wants to spend money on a publication unless they consider it will be of benefit to them. With ISACA publications you can't pop along to your local book shop for a sneak preview, but have to accept on trust that the publication will meet your needs. We have debated a number of solutions ranging from the proverbial 'do nothing', to holding a complete set of publications for display and viewing at our meetings. This last option is prohibitively expensive and would only be of use to the ten percent of you that attend our meetings. It would also involve us in storage and security problems - oh yes, we have had publications lifted from under our very noses in the past! The 'do nothing' option doesn't appeal either, so we have come up with a couple of compromises. First, I have sent an enquiry to International to ascertain whether they will let us have a complete set of publications for 'marketing' purposes. Don't hold your breath over this one, because if they do it for us, then the other 120 Chapters will be climbing on the band wagon. Second, we are going to start publishing reviews of ISACA publication in Datawatch and on our web site, so that you can at least draw on the experience of others before committing your hard-earned cash. There is however a problem with this wheeze - getting the reviews in the first place. Some we can lift from other sources, but others will have to be produced by .....YOU! So here's the two edged sword. Lifting the IIA's motto of 'progress through sharing' and abusing John F Kennedy's famous quotation, 'ask not what your Chapter can do for you, but what you can do for your Chapter', I am appealing on behalf of your colleagues, and your editor, for you to put pen to paper regarding any ISACA publication that you have read recently. If you are CISA qualified it also counts towards your annual CPE hours. So you budding Jane Austen's do your bit for your Chapter and make your contribution to the greater good of IS Auditing.

IT Governance is the new name of the game and ISACA has created an IT Governance Institute (www.itgovernance.org). Having been deeply involved in creating an IT Governance framework for a global enterprise I was excited by this new development of our Association. The web site is really useful and I urge you to visit it. Paul Williams, the International President (and previous President of this Chapter) gave a presentation on the subject to members of your Management Board last month. We had a lively, but positive and constructive debate and I believe that Paul was well pleased with the favourable reception of this initiative. This subject is so important that it may well form the theme for next season's programme of meetings, but don't wait until then. Visit the web site now!

London Chapter Events

16 March 2000
Digital Signatures
Fred Piper & John Mitchell

20 April 2000
Intrusion Detection
ISS

18 May 2000
AGM &
Penetration Testing
Steve Bailey

15 June 2000
Contingency Planning for the Extended Enterprise
TBA

All meetings will take place at the offices of KPMG, 8 Salisbury Square, London EC4 commencing at 4.30pm. Meetings are free to members, a charge of £20 will be made to non-members.

Government issues wake-up call to UK Business

By Allan Boardman

UK e-commerce transactions in 1999 are expected to be worth around 2.8bn and predicted to grow tenfold over the next three years reaching 4% of total UK GDP by 2002.

This suggests a relatively small percentage. However, the true contribution to the economic welfare of the country is much more startling, as e-commerce tends to put downward pressure on inflation and increases economic growth. Figures published by the US Department of Commerce suggest that in the years 1995 to 1998 the Information and Communications Technology industries, the key enablers of e-commerce, were responsible for 35% of US real economic growth, whilst representing only 8% of US GDP. In 1996 and 1997 these industries were believed to have lowered US inflation by 0.7%.

In September 1999, Prime Minister Tony Blair issued a wake up call to UK industry and commerce to embrace and exploit e-commerce. Conscious of the immense opportunities and threats posed by e-commerce, the Performance and Innovation Unit (PIU) of the DTI prepared a strategy to make the UK the world's best environment for electronic commerce.

The PIU report identified three areas in which the UK needs to make progress:

- Facilitate access to technology and networks
- Enhance the understanding of the potential of e-commerce
- Create an environment where people can have trust in the new medium

The report found that the UK has key underlying advantages in exploiting e-commerce, including:

- The English language predominates the Internet; it is used on 80% of the websites world-wide;
- a liberated and competitive telecommunications market;
- a track record of deployment of new technology, for example interactive digital television, multimedia mobile communications and pervasive computing;
- major strengths in broadcasting and content industries.

Despite the obvious advantages, the UK lags behind the major economies of the US, Canada and Australia on measures of both business and consumer e-commerce. In Europe the UK is way behind smaller Scandinavian countries such as Finland, Sweden and Norway. Germany and France are catching up fast.

To get the UK to more fully harness and exploit e-commerce, the PIU came up with 60 detailed recommendations, some of which are already underway. Full details of the recommendations can be found at: www.cabinet-office.gov.uk/innovation/1999/ecommerce. There is a lot for IT security, audit and control professionals to chew on in this report.

Allan is a Chartered Accountant and CISA and runs his own e-Business consultancy called Internet Working 4U - www.internetworking4u.co.uk

London Chapter's New Website

A member recently told me that he had visited the Chapter's web site only once in the last year, "I have no reason to visit the site!!" were the words to be more precise. Well, we have obviously failed in this instance.

The site is there for the benefit of all the members and an excellent mechanism for sharing ideas, information and knowledge. But then I would say that. Perhaps a bit of an insight into the web site will help to persuade the aforementioned member to change their views.

These are some of the things that have been added recently:

- Internet Links - links to web sites that may be of interest to members
- SIG pages - diary of events and slides from recent presentations
- Slide presentations from monthly Chapter events
- Administrative forms including CISA review course and membership application forms.

During March the site will be moving to a different hosting service that provides us with more web space and allows us to add some additional features. From a visitors perspective, the old address: http://members.aol.com/isacalondn will no longer be in use and the best way of getting to the site will be via the ISACA UK site www.isaca.org.uk and following the link to London. Nancy's email address will change to nancy@isaca.org.uk.

Once the new hosting service is in place, it is planned to have an area restricted to members where we can share ideas, experiences and information, and participate in discussion forums. It is also planned to provide for online bookings for Chapter events and SIG meetings.

I would like to take this opportunity to make a request to members to let me know if there are any changes they would like to see on the web site. Perhaps something you have seen elsewhere on the web or something that works in your own organisation. It is often the simplest of ideas that have the most impact. A recent suggestion was to include details of articles from past Chapter Magazines. This will be done soon. Happy surfing!

Enterprise Oracle Security Management

By Karen Nelson, Insight Consulting

Relational database systems have become a mainstay for building and integrating applications, such as Enterprise Resource Planning, Customer Support Management and business-to-business Extranets.

Corporate departments have discovered that they can outsource development of Internet-based applications with minimal assistance from IT. Without an appropriate security management plan, valuable corporate databases can be exploited resulting in loss of confidentiality, availability and integrity. Responsibility for security may be not be clearly defined. Contracts for services from ISPs, Web Hosting and development services, and online credit providers may fail to adequately consider security requirements.

Using the specifications identified in British Standard BS-7799 Parts 1 and 2, Information Security Management Code of Practice and Specification respectively, an information security management plan can be designed to assist end user managers, security and audit management, coordinate the security interest of their company database applications and outsourced web solutions. C:cure certification may be sought for all or portions of the system. For example, if the company's objective is to increase consumer confidence in the delivery of an Internet channel, the company may want to certify the web-based portion of the application. If the objective is to ensure that data in databases used for business-to-business Extranets is not exploited by competitors, the company may want to include certification of security controls over database system. If the company wanted to ensure that security weaknesses in trading or business partners systems would not compromise their own, they may benefit from some type of mutual certification agreement.

The Information Security Management Specification identifies and organizes areas that typically require planning and selection of security controls. It emphasizes selection of appropriate controls based on risk assessments, business requirements, legal and contractual obligations. It requires the organisation to qualify and substantiate the requirements for the controls selected in a "Statement of Applicability." While the standard identifies specific controls, it expressly suggests including those from other standard organisation bodies, such as ISACA's COBIT, IIA's SAC, and InfoSec's Common Criteria. If SAS-70 or WebTrust reviews are selected as controls, they become part of the Information Security Management Plan used to substantiate the organisation's security management framework. The information security management specification is not limited to technical controls, but includes procedures and practices that would attempt to prevent "social engineering," other "soft" offenses or careless practices.

The remainder of this article will address many of the technical security controls designed into the Oracle database system that should be evaluated when implementing security plans or auditing database security. The Oracle database system has a strong security architecture designed to offer both mandatory and discretionary security controls. Its security options range from moderate to high, and may be implemented to meet most business requirements for security. In order to select the level of security control most appropriate for the system, the first step is to identify the business objective of the system and associate all the assets used to deliver this service. A thorough risk assessment will show the impact to the business of failure to meet service delivery requirements. The organisation's information security policies and standards for Oracle security, along with the results of the risk analysis, will determine the extent of control required. When an organisation has not established standards the reviewer may need to recommend best practices suitable for the application. The reviewer can then perform a 'Gap' analysis to determine the extent of deviation from the required goals and actions required to ensure an appropriate information security management plan. The Standard emphasizes selection of the best controls; this may require elimination of ineffective or unused controls.

Figure 1 illustrates a typical Extranet solution. Under the Standard an organisation could

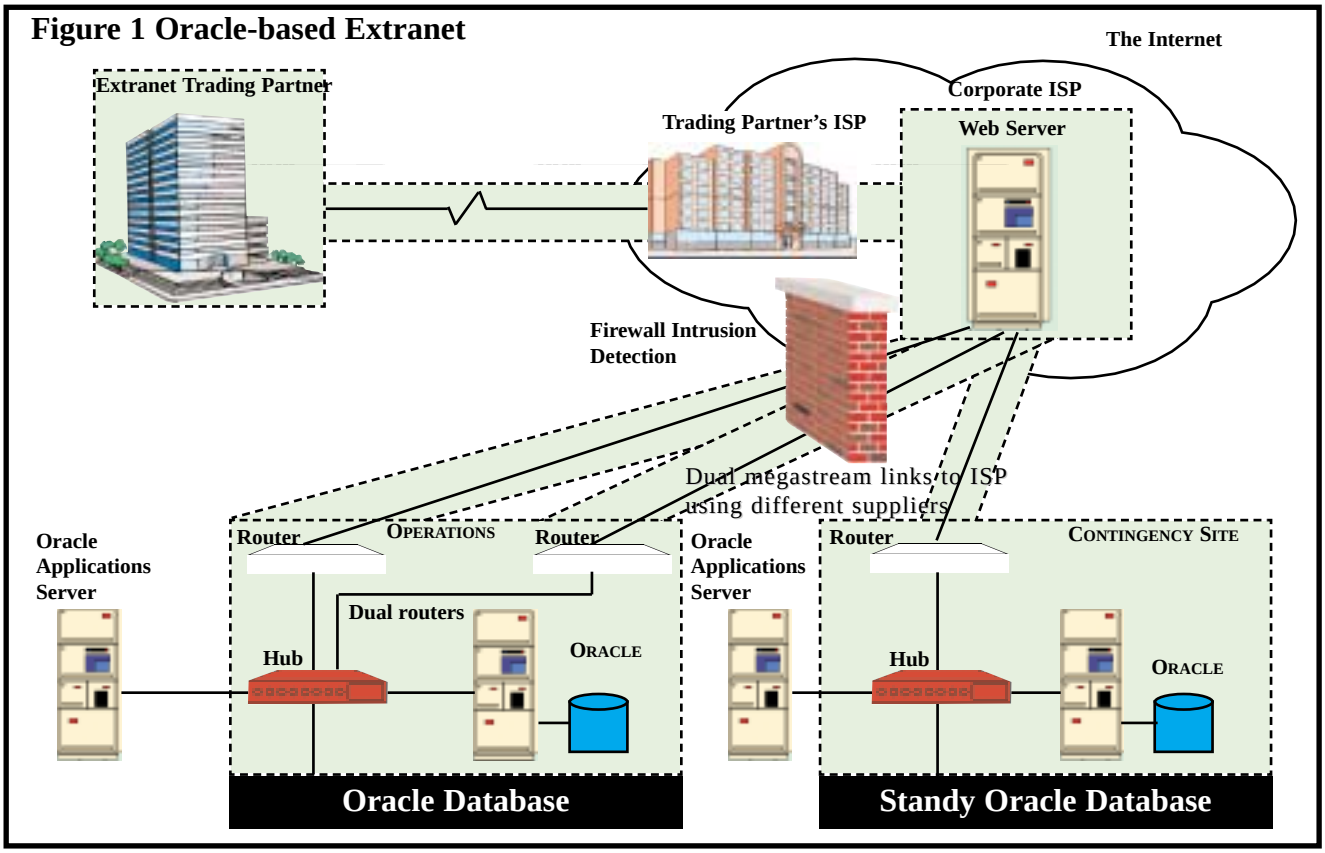
choose to certify the entire Extended Enterprise solution or break it down into smaller projects, such as the online credit or payment process, the Internet delivery channel, the Web server acting as middleware, or the backend databases and other solutions.

Additional complications and vulnerabilities occur when highly trusted users configure the database to pass through database authentication and privileges in their operating system accounts. To ease administrative burdens of being asked to serve as both operating system administrator, DBA, and Security Manager, the highly trusted user group may use a "ROOT" or superuser account along with "trusted" links to manage multiple databases on multiple servers with a single logon. By compromising a single account, security in all database application systems could be severely compromised and undermined. Interlopers target these types of accounts. Once captured the accounts can be used to create backdoor, highly privileged accounts, manipulate, expose, or destroy data, cause denial or disruption of service, erase audit trails, and issue unauthorized commands.

database management system offer more than four different authentication methods, ranging from weak, i.e., logging in without a password, to strong, using encryption. Depending on the method selected requirements for implementation must be appropriately managed to provide the level of authentication intended. The four methods include the following:

1. Database Authentication;
2. External Authentication;
3. Enterprise Authentication;
4. Advance External Authentication through the use of encryption, tokens and biometric devices.

Figure 1 Oracle-based Extranet



Responsibility for Security

When evaluating security in an Oracle database management system, first establish who has responsibility for security. Often responsibility has not been explicitly assigned and security management is an implicit responsibility of the Database Administrator (DBA) or a pool of DBA's. In larger organisations, a position maybe defined as Security Manager or Systems Administrator. Frequently Oracle applications developers obtain DBA privileges, which they fail to relinquish when the database goes into production. Although Oracle offers a robust role-based system for designing and segregating special privileges required for highly trusted users, these features may not be employed.

Authentication and Password Management

New releases of the Oracle database management system offer more than four different authentication methods, ranging from weak, i.e., logging in without a password, to strong, using encryption. Depending on the method selected requirements for implementation must be appropriately managed to provide the level of authentication intended. The four methods include the following:

1. Database Authentication;
2. External Authentication;
3. Enterprise Authentication;
4. Advance External Authentication through the use of encryption, tokens and biometric devices.

Database Authentication

Under database authentication, the Oracle database system is used to manage user accounts, passwords and logon authentication. The users are not required to have an operating system account. New features in Oracle version 8 permit the use of the following controls:

✦ Automatic timeout after so many

minutes of inactivity;
- ✦ Automatic account lockout after a specified number of unsuccessful logon attempts;
- ✦ Account expiration;
- ✦ Forced change of passwords;
- ✦ Forced use of hard-to-guess passwords;
- ✦ Notification of pending password expiration;
- ✦ Inability to reuse passwords for a certain number of days or until a certain number of password changes have been made;
- ✦ Encryption of passwords in storage and at logon (only when appropriately configured);
- ✦ Automatic specification of "quotas" that would prevent careless or intentional tying up of resources which could result in denial of service.

The default profile must be changed in order to make the options listed above mandatory and initialization parameters on the client and the server must be set to ensure password encryption.

External Authentication

When supported by the vendor implementation, the operating system can be used to manage user accounts and logon authentication, role assignments and/or collection of audit data. By setting the OS_AUTHENT_PREFIX=value, the user will be able to connect to the database using the operating system user account and password. When the connection is attempted, Oracle checks that the Oracle user account matches the requesting operating system account. However, by default, Oracle does not permit this type of authentication over unsecured networks, such as Oracle's SQL*Net or Net*8. For remote login over insecure connections are not a concern, the Oracle system must be configured to permit remote OS authentication login. External authentication is frequently selected to avoid multiple sign-ons. However, this type of authentication exposes both the operating system and Oracle database to vulnerabilities related to unauthorized access. Therefore, effective operating system-based user account and password controls must be employed in these situations.

Enterprise Authentication

In Oracle 7.3 and later versions, Oracle has provided the Oracle Security Server (OSS) which can be used to support single sign-on authentication. With this system the OSS administers password management and authentication. The OSS serves as a central repository for global user accounts and global roles. Distributed database servers and clients must register with and receive a public key X.509 certificate from the OSS server in order to be "trusted." Instead of using passwords, when a client connects to a server as a global user, the server verifies the global user's identity with the Oracle Security Server. The certificate and private key stored within the client "wallet," must be protected from unauthorized access by the operating system. On some platforms this may result in unacceptable exposure. Therefore, Oracle has provided additional advanced networking options.

Advanced External Authorisation

Oracle advanced networking provides Oracle authentication adapters for third party applications and hardware devices, such as SecureID's security token, Identix TouchNet II - biometric authentication adapter, Kerberos and CyberSAFE Challenger network authentication, and DCE authentication adapters.

Both the client and server can be set up to use multiple types of the authentication adapters listed above. Each service requires the installation of product-specific toolkits, servers, and hardware and network configuration parameters. The Oracle Advanced Networking Option uses the Diffie-Hellman public-key key negotiation algorithm for key distribution; MD5 message digest algorithm; DES40, DES, RC4_40, RC4_56, and RC4_128 encryption algorithms.

Access

To control access to schema objects and execution of system processes, Oracle requires that user accounts be assigned privileges. For example, to connect to the database, the user must be assigned the "CREATE SESSION" privilege. Assignments of privileges can be made explicitly through grants to a particular user, or through grants to ROLES, which may then be assigned to users with similar requirements. By default, the DBA role has the "Grant Any Privilege."

System Privileges

Privileges may be classified as SYSTEM privileges and OBJECT privileges. Oracle 8 has over 60 specific system privileges, ranging from starting and shutting down the database instance to creating tablespace or deleting rows in all tables. Certain schema objects, such as clusters, indexes, triggers, and database links, may only be accessed through granting of system privileges. System privileges are normally assigned only to highly trusted user accounts whose responsibilities include database maintenance.

Object privileges

Access to tables, views, sequences, procedures, functions, packages is controlled through the use of schema object privileges. When used with tables, Object privileges permit security of data manipulation language (DML) functions and data definition language (DDL) functions. Table 1 list commands that can be assigned.

Table 1. Access to Tables and Other objects

DML Operations	*DELETE, INSERT, UPDATE, SELECT*
DML Operations	*ALTER, INDEX REFERENCE*

Most DDL operations should be limited to highly trusted users. For example, users with the ALTER USER command can use the privilege

to impersonate another user. The EXECUTE privilege can be assigned to users to force access to objects referenced in a procedure through execution of the procedure. The procedure runs under the privileges of the user who owns the procedure regardless of who executes the procedures. Users, therefore, do not have to be granted as many privileges.

Roles

Roles allow grouping of related privileges that can be assigned to users or other roles. Roles should not be used with application developers; the privileges to access objects within stored programmatic constructs need to be granted directly. Roles make it easier to manage end users. Certain roles and privileges should only be granted to highly trusted users, such as DBAs, Security Managers, and technical support staff.

Another common use of roles is to control database applications. The application role is assigned all privileges necessary to run a given database application. The role is then assigned to users or other roles. Several different roles may be defined for an application in order to restrict access according to various requirements. Users who require access to the application are assigned a role that meets their requirements.

Intrusion Detection & Monitoring

When password management features are used in Oracle 8, the database will automatically lock out accounts that exceed the threshold for unsuccessful logon attempts. The account will remain locked for a specified number of days when the FAILED_LOGON_ATTEMPTS has been exceeded. Only a DBA account can unlock the account using the ALTER USER command.

Oracle has its own Audit facility, however, it often is not enabled. The audit table is part of the SYSTEM tablespace and must be protected from unauthorized access. By default users can access their own records. Audit procedures and techniques must keep the audit database manageable while providing limited but useful information. When suspicious activities are detected, emergency audit procedures that provide more detail can be invoked. The operating system logs certain events by default, such as Oracle instance shutdown and startup, and connections to the database as the administrator. The Oracle views containing audit information that must be extracted using SQL. The audit tablespace must be maintained to prevent performance degradation. In addition to Oracle third-party products also may be used for monitoring and auditing Oracle security.

Recovery and Backup

The database is usually a component requiring 100% availability, making recovery and fault tolerance as essential as backups. Essential database components include the hardware, software, network, process, or system. Hardware devices often used include RAID storage devices, standby databases, mirrored storage and media storage. Special considerations must be given in Oracle for multiplexing specific files and for archiving data files. "Damage to a non-multiplexed online redo log causes database operation to halt and may cause permanent loss of data," according to the Oracle. Other special files critical in recovery include rollback segments and control files. Initialization parameters can be set to ensure automatic backup of all required files. Oracle offers several alternatives for backing up databases including high availability, standby databases. Backups can occur offline or online. Oracle offers the Recovery Manager Database Utility to automate recovery and backup. Oracle recommends running Recovery Manager from a separate server.

The Environment

UNIX-server based databases comprise the largest share of the SQL database market. Special requirements for the use of the ROOT account occur during installation, and the Oracle installer creates the UNIX account "ORACLE," to become the owner of the Oracle software distribution. No other use of the ORACLE account should be permitted. The Oracle installer also relies on the creation of special UNIX groups, OSOPER and OSDBA (which may be named differently), to use in granting special user database privileges and in security files and libraries. Two database accounts created at installation, SYS and SYSTEM, come with well-known default passwords, which should be changed. These User-Ids own the system tablespace and data dictionary and operate with high privileges. Once the accounts are created the installer can automate creation of files and directories with recommended access permissions. During configuration Oracle recommends that the DBA verify appropriate permissions have been placed on files and directories.

Conclusions

While Oracle offers many options for securing and recovery of its database applications, having an Information Security Management Plan will ensure that those features required in your organisation have been enabled and deployed. The c:cure scheme is especially useful when the organisation needs to coordinate information security management plans at globally dispersed sites and when the organisation wishes to establish customer or client confidence. Good security practice demands that full cognisance is taken of the business requirements, the potential impacts of security failure and the capabilities of the system. This ensures the implemented services achieve the correct balance between usability and data protection.

Karen is a consultant specializing in database security. She is a CISA, CIA and a Certified Microsoft Professional. She is a member of ISACA and the IIA. She has worked in information security and audit for the past 12 years for several Fortunes 500 companies and non-profit organisations.

NETWATCH

By Annabel Lane, Nestle UK Ltd

My boss called me in the other day to his office, fixed me with that look and said "This ecommerce thing - what should audit be doing to get involved?"

A very good question. No doubt those of you who have been attending the extended enterprise series of meetings the chapter has been holding this season could answer that one very quickly. I had to bluff a little bit and promise to come back to him after I had done some research. So I was straight onto the internet hunting around for information I could use to blind him with science. Some of the results I thought I'd share with you.

Roger Clarke's Electronic Commerce
http://www.anu.edu.au/people/Roger.Clarke/EC

This is a very comprehensive site, starting right from basics on how the internet works and what ecommerce is. Of course we all think we know all about that but you start trying to explain it to your maiden aunt Maggie and you'll probably find there's a lot you take for granted. This one's a little out of date but the papers Mr Clarke himself has provided are very good and clear. They range from introductory papers on key terms, EDI, internet technology, privacy and so on, right through to more detailed advanced papers on more specific relevant subjects such as Mondex and PKI. There are also a huge range of links to pursue.

Ecommmerce Info Centre
http://www.ecominfocenter.com

Here's another one with more information than you could possibly wish for. It describes itself as a one stop shop regarding ecommerce and has over 29,000 selected links. A lot of it is general to ecommerce in business and gives some information on the commercial and business implications. Quite useful for those of us who normally have our noses so close to the technical grindstone that the commercial realities fade into the distance! If it's further links you're after, scroll down the page for areas such as the economics of ecommerce which links you into a page with a picture of Adam Smith and a list of categories like Privacy and Law, Security, Privacy and Encryption, Intellectual Property and so on.

Clicking on these links in turn takes you to further lists of sites. This site describes itself as the ebusiness portal and there's definitely a ton of information here although I found it a bit hard to navigate around.

Infosecurity 2000
http://www.infosec.co.uk/page.cfm

This site is specifically set up to promote the infosec conference and has loads of articles on the whole information security area on it as well as just being set up to promote the show with information on the exhibitors and products available. I particularly liked the fact sheets which cover areas such as Biometrics, Encryption, Internet Security, BS7799, etc. Check out the general information - 24 frightening facts is especially interesting. Apparently only 8% of businesses with no disaster recovery plan ever reopen following a disaster. Now that's something to frighten recalcitrant IS managers with!

Computer and Network Security Resource
http://www.infosyssec.org/infosyssec/index.html

This site was recommended to me by a member (so thanks are due to David Ward). If you can't find what you're looking for on this one then it probably doesn't exist. It's so comprehensive it makes an excellent starting place for any kind of information you require on information security. I could write a whole Netwatch article about it alone! Yahoo described it in January 2000 as "The most comprehensive computer and network security resource on the internet for Information System Security Professionals".

The first area of information on the top left points you in the direction of what they call "Our research resources. This takes the form of a huge list of topics on an A-Z listing and includes Cellular Communications, Firewalls and the Internet, Hacking - How it's done guides, Linux Resources, Penetration testing, you name it. Clicking on one of the titles takes you to a page devoted to that topic, for example as I am supposed to be looking at ecommerce this issue, I clicked on the firewalls title. This took me to another page of more links, commencing with general information licks, such as "how to pick a firewall", "firewall FAQs" etc and then going on to Firewall company websites, Firewall industry guides and more useful links such as firewall 1 tips and hints.

The next header along is for a bunch of sites dedicated to daily updates of system alerts, exploits and vulnerabilities. Some of these are old favourites of this column ,such as CERT and CIAC, but there are plenty others to look at for recent bulletins on vulnerabilities and viruses that have been exposed. Beneath this section there are also vendor issued notifications of alerts and patches that have been issued. For example clicking on the link labelled "Microsoft Security" - I know some of you out there will be pointing out to me that this is an oxymoron - you are transported to Microsoft's Security advisor page, listing its security bulletins.

More daily updates are provided under the heading of security news sources, where there are links to conferences and other events, Linux news, even UK Hacker news which has some interesting articles within it though the black background did put me off rather!

Virus and trojan alerts also make a section with links to the current top ten virus alerts from Sophos and databases to search - you can actually enter the name of the virus on this web page and it will search the relevant site and take you straight to the definition. Very useful for all those mail messages about dastardly viruses well meaning friends keep sending me! If rather than a virus it's a security topic you're looking for, try the Altasecure dictionary provided. This works on a similar principle but be warned - make your queries specific. I entered the word "spoof" and the first web site offered to me was about Casino Royale, labelled as a James Bond spoof!

There's plenty more on search engines, underground search engines, bulletin boards (white hat ones of course!), assorted "neat" things like tools on various web sites, and if you couldn't find what you were looking for on here, you could always try linking to another site via the other listings of top sites for hacking and security which are listed here, for example, the progenic top 100. To get into this one you have to vote for this site, though it only takes a few seconds. Then you get a list of the top 100 hacking information sites.

Anyway, all in all the Computer and Network Security Information Resource is the type of site that anyone in the field of IS Security or Audit could make a great deal of use of and it's definitely my star site for this edition!

Fast Search - all the web all the time
http://alltheweb.com

I use a few different search engines these days but this is one I was recommended recently and I have found it very useful. It's supposed to be the largest search engine around at the moment with over 300 million pages indexed. It usually comes up with the goods for me and makes a good starting point for your searches. I seem to find more relevant sites via this method than any other the others I use at the moment. No doubt some of you use something better so let me know if so!

Dotcomguy: Your ecommerce guide
http://www.dotcomguy.com

Thought I'd take this one for my coffee break site this edition, though it also deals with some serious issues. Dotcomguy claims to be a normal person who has legally changed his name to Dotcomguy who decided to prove that it was possible to live off the internet for a year. He moved into and empty house and furnished it via on line purchases. Everything he buys he buys over the net. Check "How Dotcomguy survives" for a run down of how he furnished his house and got the equipment he uses - even fitness equipment! There are tutorial items on what is ecommerce and what is encryption though you won't get much out of these if you've visited the sites I've recommended previously. He keeps a daily journal and yes people do come round and visit him so it's not as sad an existence as you might imagine! Check out what's going on in the Dotcom House! And realise the potential of ecommerce!!!

And finally….

I had to share a few of these with you as I am sure they're true. After all we all know users like this, don't we…???

Tales from the help desk:

At 3:37 a.m. on a Sunday, I had just looked at the clock to determine my annoyance level, when I received a frantic phone call from a new user of a Macintosh Plus. She had got her entire family out of the house and was calling from her neighbour's. She had just received her first system error and interpreted the picture of the bomb on the screen as a warning that the computer was going to blow up.

Tech Support: "I need you to right-click on the Open Desktop."
Customer: "Ok."
Tech Support: "Did you get a pop-up menu?"
Customer: "No."
Tech Support: "Ok. Right click again. Do you see a pop-up menu?"
Customer: "No."
Tech Support: "Ok, sir. Can you tell me what you have done up until this point?"
Customer: "Sure, you told me to write 'click' and I wrote 'click'." (At this point I had to put the caller on hold to tell the rest of the tech support staff what had happened. I couldn't, however, stop from giggling when I got back to the call.)
Tech Support: "Ok, did you type 'click' with the keyboard?"
Customer: "I have done something dumb, right?"

One woman called Dell's toll-free line to ask how to install the batteries in her laptop. When told that the directions were on the first page of the manual the woman replied angrily, "I just paid $2,000 for this damn thing, and I'm not going to read the book."

Customer: "I received the software update you sent, but I am still getting the same error message."
Tech Support: "Did you install the update?"
Customer: "No. Oh, am I supposed to install it to get it to work?"

INTERNET RESOURCE LIST

AUDIT

www.isaca.org.uk
www.isaca.org
www.auditnet.org
www.acua.org
www.gallaudet.edu/~auditweb/index.html
www.gallaudet.edu/~auditweb/kits.html
www.anao.gov.au/reports.html
www.theiia.org
www.iia.org.uk
http://www.methodware.com/links/
www.itaudit.org

SECURITY

www.cert.org
ciac.llnl.gov/ciac/
spam.abuse.net
www.cl.cam.ac.uk/spam/
www.iki.fi/liw/mailfilter.html
csrc.nist.gov/secpubs/unix_security_checklist.txt
www/ntsecurity.net/
www.first.org
www.cauce.org/
http://www.securityportal.com/
http://www.antionline.com/
http://www.cerias.purdue.edu/coast/hotlist/
http://www.sse.ie/securitynews.html
http://www.infosyssec.org/infosyssec/index.html

COMPUTER COMPANIES AND SYSTEMS

www.microsoft.com
www.alw.nih.gov
ntresearch.com/
www.acl.com/audit/audit2.htm
www.cica.ca/idea/index.htm

OTHER ORGANISATIONS

www.bcs.org.uk
http://www.auditserve.com/frmain.htm
www.coactiveconnection.com/
www.mc2consulting.com/

HACKERS AND VIRUSES

www.2600.com/mindex.html
www.sophos.com/virusinfo
www.drsolomon.com/vircen
http://www.cnn.com/TECH/specials/hackers
http://www.l0pht.com/

AREAS OF AUDIT INTEREST

www.disastercenter.com/audit.htm
http://www.teleport.com/~jhw/csa/
http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm

Securing E Business

By Paul Healy, RSA Security Ltd

"The Internet is a dangerous place. I wouldn't go there if I were you..." .. **is the kind of sentiment I have heard from many people.**

Yet, like the dark cellar that the nightdress-clad heroine always ventures to with her candle, conducting business on-line is an unavoidable magnet. Marketing, sales and even finance line of business managers have all got the "DOT COM" bug. Fear is spreading that some internet start up company will take away a large slice of their market share unless they act now. Amazon.com is the classic example that is quoted by most people "in the know" about how a small company can come from nowhere to become a market leader in three years. The more research is done the more attractive it seems, some large companies now conduct the majority of their business on line, from ordering to supply chain management, with quoted savings of up to 8% on overall operating costs. European businesses are clambering over one another trying to catch up with their American counterparts before it's too late.

Just as IT and IS managers let out a deep sigh of relief that their information systems survived the millennium bug with little or no disruption to service, their line of business managers now potentially want to expose the corporate data systems to the world via a web site. The attractions of shorter development times, more efficient production, more cost effective sales operations, improved customer contact are all factors which determine a companies future, and all now seem to rely on web enabled technology for information sharing.

In theory becoming an "On Line" business sounds great, but in reality it has problems. Ask an average Internet user, and you will find that anywhere between 1/20 and 1/3 of them will not shop on-line. People believe that somehow, the Internet will suck the numbers out of their card and spread them to all the criminals on line, or that they will be personally responsible for the use of the card. If users do not trust small amounts of their own money to internet companies, how can IT and IS managers trust the internet to ensure safety of the corporate data from attack from hackers, internal staff, fraudsters and industrial espionage. For nearly all businesses the commercial value of their information systems and the data they hold significantly outweighs turnover, buildings, equity and other cash values. Information is about being number one in your market.

Solutions exist today to reduce many point computer security issues but as we move into the Web enabled world so new security issues emerge which require more sophisticated and integrated solutions. Information and computer security should no longer be considered a necessary evil and implemented just to keep the Information Security Officer happy, but as a business tool that can enable your business to operate in new ways more effectively than today.

So lets look at what has to be done in order to ensure that the company's web strategy succeeds. In order to conduct business electronically, the same safeguards have to be in place that exist in the paper world. Consider your need to transfer money to someone else, important safeguards are in place.

The cheque signatory trusts the bank that they will only transfer the money to the correct recipient. By carefully writing the amount in letters and numerals and by putting a line through un-used space, the person ensures that the likelihood of the cheque being altered is minimal. By signing the cheque the bank can verify that it is the authorised user who is transferring money. The bank ensures that the money is taken out of the correct account by printing the Sort Code and Account Number on the cheque, which is unique to that person. It ensures that the money is put into the correct account using a pay in slip, which again has a unique sort code and account number. In order to ensure that the details are not made public, the cheque is put into an envelope, which is unlikely to be opened by the post office.

In order to conduct this very simple transaction electronically, four important criteria have to be satisfied:-

1. We can guarantee the identity of the parties involved in the transaction
2. We can guarantee the information transmitted has not changed
3. We can guarantee the confidentially of the information in transit
4. We can protect against denial of transaction by one of the parties (non-repudiation)

These four criteria are routinely assured in traditional business transactions, for example when people meet face-to-face, read & sign a contract, witnessed by a third party, such as a law firm representative. However, in electronic systems, such as e-mail, or web systems, these four criteria are not so simply achieved. Solving them requires the use of

computer cryptography and unique, safely distributed keys (which can be used as proof of identity and for encryption), implemented in a vendor-independent fashion with a very, very simple user interface. Impossible? Meet PKI.

Solving the problem - PKI

PKI stands for public key infrastructure. It describes a system for managing the essential elements of cryptography to enable the four criteria to be satisfied. To understand how this works, we need to look at how encryption solves these problems.

How do we guarantee the identity of parties? By providing them with a unique key that can be used with encryption to "stamp" data or a transaction with a unique fingerprint. Since a user is the only person to possess a particular key, data stamped with that key is traceable to that that user.

How do we guarantee that the content of the message has not been changed in transmittion between parties? By distilling a unique index (a message digest) of the data to be sent and sending it, stamped with the originators unique key, to the receiver. If the message has been altered in any way, even by so little as a full stop, a completely different message digest is generated. The receiver can prove that the message digest came from the sender. This is called a digital signature. By calculating a message digest from the received and comparing it to the sent protected message digest a match indicates that the message has not changed.

How do we guarantee the confidentiality of the data transmitted? By encrypting the data so that only the receiver can decrypt it.

How can we protect against denial of transaction? By using digital signatures. Since a digital signature is unique to a user, it can be used as proof that the user originated a transaction such as transferring funds voting, or signing a contract. By digitally signing a message, transaction or form on line, it shows the recipient who issued the request or message, and guarantees that it has not been altered since that time.

This is how simple cryptography is used within business systems to satisfy the four criteria. However, this is not PKI. PKI fixes all the new problems that are thrown up by simple cryptography. For example, how do you connect a key with a user? Who's to say that this user and that key match? How does a recipient decode a sender's message, if the receiver does not possess the sender's key? And if the recipient does possess the sender's key, how do you guarantee that the receiver does not use it to impersonate the sender to someone else?

Public Key Cryptography

Three cryptographers, Rivest, Shamir and Alderman, the founders of RSA, solved the problem in the 70's by inventing a new form of cryptography, based on encryption key pairs, called public key cryptography. Each user has two keys, one which is in their sole possession (the private key) and the other freely made available (the public key). The beauty of this system is that users don't have to be aware of encryption keys at all, but instead, exchange documents of trust called digital certificates. A certificate is an electronic file generated by a trusted third party called a Certificate Authority (like the party in the contract-signing example above) and testifies that a public key belongs to the user named in the certificate. This certificate is in-turn digitally signed by the Trusted Certificate Authority, proving its validity and origin and providing proof against tampering.

Public key cryptography and PKI are deep subjects and more than a match for the space allotted to this article. If you want to read more please look at Ref 1 at the end of this document. Probably the most important thing about PKI is that it's already pervasive. RSA Security have licensed it's algorithms to the leading computer suppliers, such as Microsoft, Netscape, Sun, Compaq and Novell. Indeed the RSA algorithms have become such de-facto standards that they are already used in all secure web transactions (that little key that appears in your browser when you initiate a secure connection to a web server indicates that the RSA algorithms have been engaged).

So where else is public key encryption used? Not only in browsers and web transactions but also in secure e-mail transactions. Microsoft, Lotus, Novell and Netscape all support a standard called Secure Multi-purpose Internet Mail Extensions (S/MIME), which allows you to digitally sign and encrypt mail communications. The benefits of using S/MIME e-mail is that you can start to use mail to convey legally binding and/or sensitive material, such as contracts. Another protocol that incorporates public key encryption is Secure Sockets Layer (SSL), which can be used across TCP/IP networks to secure any client-server application such as SAP R/3, PeopleSoft, Oracle or Lotus Notes, or a Virtual Private Network (VPN). Another application for public key cryptography is in the new Wireless Application Protocol, which is being used by mobile phones, and other mobile devices for Internet access, share dealing and Internet Relay Chat. Also, look out for PKI in electronic document systems such as Adobe Acrobat or in forms software such as Informs or Shana Informed.

Physical Me, Digital Me

One problem that PKI does not really solve is the problem of who is actually behind a certificate. To illustrate this problem, think of a man who registers for home banking. He registers on-line with his bank and as part of the process, has digital credentials generated in his web browser (such as Microsoft Explorer or Netscape Navigator), he gets assigned a certificate by a certificate authority and hey, presto he is ready to go! However, the digital credentials and matching certificate are stored on the hard disk of his computer - which, while he is out, his son decides to have some fun at his dad's expense, makes some transactions and increases his pocket money. How would the bank discriminate between the honest transaction of the father and the fraudulent transaction of the son? The

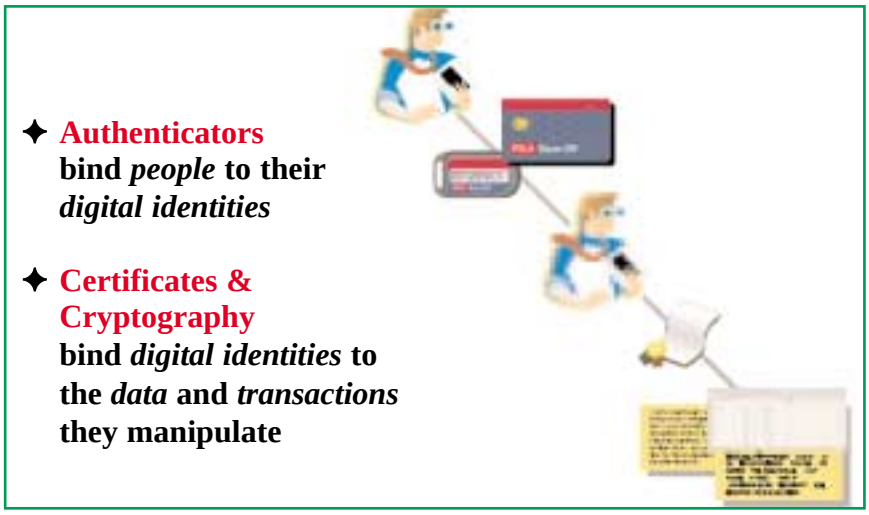
answer would be that the bank doesn't know - it's up to the customer to protect his digital credentials. With the likelihood of digital signatures becoming legally binding in the near future, this could present serious problems in a business context.

So there are more to safe transactions than certificates, encryption and keys. One useful model for this is to think in terms of two user entities. I call the first user the physical me. The second user is the digital me. The physical me is the biological entity that logs onto the computer and uses the machine. The digital me is the on-line entity I assume to manipulate data and perform transactions. The process that binds the physical me to the digital me is called authentication. The components that bind the digital me to the data I use and the transactions I perform are certificates and cryptography.

It is important to understand that the strongest systems are hybrids of strong authentication systems and PKI. Strong authentication systems usually replace static passwords with a device such a specialist protected smart card or token. This strengthens the security of a basic PKI, which usually relies on a simple password. Without strong authentication, the effectiveness of PKI boils down to the effectiveness of a password. Passwords have long been the first target of hackers to break security systems and if the trust model of a PKI is to be guaranteed, the solution should not have such an obvious weak point.

How strong is PKI? Encryption strength

Codes, like rules are made to be broken. All encryption codes can (theoretically) be broken, if you have enough time. In the real world this translates into one thing - computer power. The cryptography behind PKI is very strong - you need a lot of computer power to break modern codes. How much power do you need? This really depends on the length of the encryption keys. Your public/private keys used in digital signing are going to be either 512 bits long or 1024 bits long. A different encryption system is used in SSL, which has characteristic key lengths of 56 bit or 128 bits long. To give you a sense of how hard it is to crack, a message encrypted with a 56 bit key took 10,000 Internet-connected computers a day to crack (RSA Conference Challenge, 1999). However, Moore's law shows that every 18 months, computer speeds double, therefore we must similarly make encryption harder to crack. Fortunately, we can double the strength of encryption by using keys which are 1 bit longer, e.g. 57 bits would take 2 days, 58 bits 4 days, 59 bits 8 days, … and 128 bits would take 10,000 interconnected computers two hundred thousand billion years to crack! The question that should be asked is how long it would take to break the password that controls the access to the digital identity, if weak authentication is used? This can be minutes, hence only good e-Security uses strong two factor authentication to protect the keys.



The law and PKI

Because PKI solves the four criteria so well, it is the core technology behind e-commerce law. Most European governments are looking at implementing digital signature law, whereby electronic contracts can be made binding in law. All systems require the use of PKI. For more details please see Ref 2 at the end of this document. Effective digital signature laws will vastly accelerate the introduction of electronic commerce, for a range of transactions much greater than demonstrated by credit-card purchases.

The Future

PKI is a core technology for the new millennium as it is fundamental for enabling trustworthy electronic commerce. Companies are already realising that whatever they install will have to interoperate with the systems employed by their partners, suppliers and customers. Users want one identity to seamlessly integrate with multiple applications. Mechanisms are being requested so that users can be mobile between different base stations and access their credentials centrally. Existing non certificate friendly applications like Oracle and SAP are becoming more important to secure, as these manage and contain a large proportion of companies critical data resources.

PKI is starting to be used as an effective single sign on solution, for allowing customers to use on line help desks, for securing email and much much more. The days of a just say no security policy are over and finally security solutions like PKI enable businesses to embrace electronic commerce and still sleep at night!

For more information of how PKI works please visit www.rsa.com
For more information on the legal aspects of PKI please visit www.europa.eu.int

Telephony Security - Toll Fraud

By Duncan McKerracher

In the August edition of Datawatch, we described the four issues of telephone security - Toll Fraud, Denial of Service, Corporate Embarrassment and Phone Tapping. I hope to describe the latter three issues in future editions of Datawatch. This article concentrates on the most significant issue, that of Toll Fraud.

Toll Fraud is where a hacker makes fraudulent calls at the expense of a company or organisation. There are three main ways in which this can be carried out. These are as follows:

✦ Direct Inward Subscriber Access (DISA) is a facility available on a PABX that allows callers to make an inward call to the PABX then dial a remote telephone number. The owner of the PABX meets the cost of the second part of this call (i.e. the call to the remote telephone number). DISA is intended to be used by staff working from home who have to make a large number of international, national or mobile calls without the remote worker having to bear the cost of these onward calls. A particular extension number can be configured to be the DISA extension. Thus any calls to this extension provide secondary dial tone to the caller. The PABX can be further configured such that the caller has to enter a PIN and/or account code before the remote telephone number is dialled. However it also provides a way in which an unauthorised user can make calls at the company's expense. For this reason it is very important that the DISA facility on the PABX is properly managed and its usage closely monitored.

✦ Recorded Announcement Devices (RADs) allow calls to be answered automatically without the need for human intervention. In many cases, a RAD gives the caller the opportunity to key in certain digits to allow them to select a specific department or extension. If a RAD is not properly configured, it can be possible for a caller to key "9" thus making an external call. Many companies have fallen foul of this practice in recent months.

✦ Social Engineering is the term describing where the hacker uses the services of the telephone operators to hack the network in a more productive way. One feature of Social Engineering is where the hacker makes long distance calls, ironically with the help of the on-site operator. This is done by direct dialling a random extension within the DDI range then asking to be transferred to the internal operator. The hacker then asks to be connected to a long distance number of his choice, which the operator duly does, because it is seen as an internal call. Alternatively a hacker might ask for "extension 9155" (i.e. international directory enquiries) which will allow him to make an international call.

The following are real life examples of such Telephone Toll Frauds:

Local Authority, Home Counties

For many years this Council had a private link into a cellular network to allow its mobile staff to make calls to office staff without incurring a major expense for the call. Basically it allows the mobile phone user to dial a code to access the Council's PABX then dial the extension number of the person they wanted to speak to.

A professional hacker discovered that by dialling the code for the Council followed by '9', then an international number, he could call anywhere in the world from his telephone at the expense of the Council. This fraud continued for more than 3 months before it was detected. By this time the cost to the Council was over £160,000.

Government Department, London

A professional syndicate discovered that it was possible to dial into the organisation's PABX in London and make free calls to any destination in the world at their expense. The total cost of this toll fraud was put at more than £1million.

The fraud itself was perpetrated by using the Direct Inward Subscriber Access (DISA) feature common to many modern PABXs. It is intended to allow remotely accessing users the ability to make calls to their own organisation at company expense when working from home. Such facilities are usually password protected. In this case however a combination of poor password control and insufficient call logging analysis led to fraud on a massive scale. The perpetrators have never been prosecuted.

Higher Education Establishment, Home Counties

A higher educational establishment suffered serious financial loss and acute embarrassment due to fraudulent payphone activity perpetrated by some of its overseas students.

Students found that by tapping

into the lines of certain types of payphone that were directly connected to the University's digital PABX, they could make free national and international calls at will. Losses of £50,000 were estimated before the fraud was detected. The network operator showed no inclination to accept responsibility as the cabling the payphone and the PABX all belonged to the University.

It subsequently transpired that this establishment was by no means the only University to suffer from telephone toll fraud. Since then all University telecoms managers have been warned to be aware of the dangers.

DIY Chain Store, Wales

A DIY Chain Store used a Recorded Announcement Device (RAD) to "front end" their paint ordering service. This service allows shop owners to enter a digit (1,2,3 or 4) to enable them to be answered by a call centre based in their locality. It was discovered by an enterprising shop owner that by entering "9" the inbound caller had unlimited international access. Approximately £40,000 worth of illegal calls was made at the store's expense before the fraud was noticed and rectified.

In subsequent issues of Datawatch I hope to explain the other main vulnerabilities - Denial of Service, Corporate Embarrassment and Phone Tapping. Perhaps if you have not carried out a review of your telephone security, now is the time to do so.

Duncan McKerracher BEng is an independant Telecoms Consultant specialising in Fraud and Security issues. He is a member of the Telecommuncation Manager Association. He worked in the Ministry of Defence for over 10 years an has since helped more than 50 large companies combat telecommunications fraud

Special Interest Groups (SIG)

The principal objective of a SIG is to advance member's knowledge on a specific area of interest.

It is a particularly good forum for personal networking and advice & information. SIGs offer the chance to hear experts in their field, the chance to download previous presentations from our website (www.isaca.org.uk :check out the last three Network SIG presentations), read related articles in Datawatch and potentially produce an ISACA publication.

The London Chapter currently has three active SIGs. The Network SIG has been established for three years holding some four to five meetings per annum. The Fraud Prevention SIG has recently been formed with its inaugural meeting on the 24th February 2000 and there is Risk SIG which is in the process of being formed. Of course SIGs have a finite life and some have come and gone (e.g. UNIX SIG).

The Chapter encourages the formation of SIGs and if you have any thoughts in this direction please contact either of the SIG Co-ordinators (John Hunter or Bill Hawkins). The formation of a new SIGs is always carefully considered and a recent member suggestion for a SAP R3 SIG was not successful because of the number of quality groups already in existence outside the Chapter. Of course a SIG does not run itself and at a minimum a chairman is required for all the associated organization and administration.

SIG meetings are now widely advertised within our own community. For the SIG meetings of the 24th and 29th February (Fraud Prevention and Networks respectively) members were notified through Mailshot, e-mail as well as being publicized on our website. This new combination has proved very successful with both meetings being over subscribed.

Finally, the chairman of both current SIGs would welcome suggestions on topics that you would like to see addressed, so please do not hesitate to contact either John (Fraud Prevention) or Bill (Networks).

Bill Hawkins, SIG Co-ordinator
020 7332 1296,
bill.hawkins@corpoflondon.gov.uk

Fraud SIG

The initial meeting of The Fraud Special Interest Group was held at the offices of CCF-Charterhouse under the Chairmanship of John Hunter (of HLB International), and attended by about 20 people. The participants came from a wide variety of institutions both public and private. The first meeting was a brainstorming session to define the group's functions and objectives.

A lively, wide ranging and interesting discussion ensued, which covered topics such as how fraud should be defined, and how to distinguish Internet fraud from Internet security in general. The most popular topic was e-commerce fraud.

The group set itself the objectives of producing a set of guidelines to be published either as a booklet of as a set of web pages.

It was agreed that the next meeting of the group seek to identify individual areas of study by performing a risk analysis on the various aspects of fraud, and that to meet its objectives, the group would have to meet on a monthly basis. The next meeting of the group will take place on 23rd March, though the venue has yet to be confirmed. Details will be circulated to those who have already expressed an interest in this group. Any others who are interested should contact John Hunter via mailbox@jhunter.u-net.com

Joseph Wright (Crédit Commercial de France - London Branch)

The Big Number Change

By Bill Hawkins

I wrote an article in a previous issue of Datawatch (Volume 41 Summer 1999) on the issue of the telecommunications 'Big Number Change'. This article is a further reminder of what actions must be taken by Telecommunications Managers and/or other appropriate personnel.

The 'Big Number Change' potentially affects all aspects of your communication system including the PBX switch, standard telephone number, helpline emergency numbers, automatic systems containing programmed numbers, telephone numbers stored in databases, modems, mobiles, pagers and alarm/security systems.

Oftel decided to overhaul the telephone numbering system because the UK was running out of numbers due to the large increase in telecommunications usage in the last few years. The changes will generate hundreds of millions of new numbers affecting geographical areas, mobiles, premium rate numbers and reserving many codes for future use. This translates into a new family system of codes ranging from 00 (international) 01 (existing area codes), 02 (new area codes), 03 to 06 (reserved for future use), 07 (mobiles, pages and personal numbers), 08 (freephone and special rate services) and 09 (premium rate services).

Oftel have decided to fully introduce the new 02 codes to six areas on the 22 April 2000. These areas are Cardiff, Coventry, London, Northern Ireland, Portsmouth and Southampton. The new London code that will replace the existing 0171 and 0181 codes is 020. All existing local London numbers will be increased from seven digits to eight digits. This means that a London number that is currently 0171 332 1296 will change to 020 7332 1296.

The new dial codes have run in parallel with the old existing codes since the 1st June 1999 but currently only work when used with the full dial code (i.e. 020 7). The new local London numbers will not work alone until the 22nd April 2000. After which the old seven digit local numbers (332 1296) will not work but the full old digit code (0171 332 1296) will run in parallel but fail after the switch date of autumn 2000. The actual switch date, for new and old national codes, being dependent on location (e.g. 5th August 2000 for Cardiff, 14th October 2000 for London).

An area, which in my experience is often neglected, relates to the changes affecting mobiles and pagers. These changed on the 30th September 1999; when they were given a new 07 number, the old and new numbers can be used in parallel until April 2001.

Actions for the organisation

Each organisation should have a strategy on this matter. This will include nominating a person to manage the project, establishing how the organisation's numbers and business partners/contacts numbers are affected and establishing the key implementation dates.

Potential areas affected

- **Materials & Publicity**: stationery, advertising, promotional material, signage & livery, website, helpline and emergency numbers.
- **Switchboard / PBX / Alternative network routing**: call forwarding /barring, call loggers, alarms/ security, teleconferencing, ISDN (including CLI and international), modem (e-mail/internet/laptops), telephones/mobiles/pagers/fax machines and private payphones.
- **Records & Databases:** all records and databases (both paper-based and electronic).

Much of this article is based on the information supplied by the 'All The Phone Companies Together'. For further information please visit their website (www.numberchange.org) or telephone 0808 22 4 2000 (free booklet 'The Big Number for Businesses').

The changes required
There are twelve required changes, with key dates as follows: -

Changes that should have been implemented prior to 1st June 1999
- Call barring
- Alternative network routing (National dialling using new 02)
- PhONEday fixes
- Private payphones
- ISDN incoming (02 areas only)
- Call management systems (Loggers)

Changes required before 22nd April 2000
- Calling line identify (caller identification)
- Routers connecting LANs
- Stored numbers (local format)
- Alternative numbers (national format)

Changes required as soon as possible after the 22nd April 2000
- Alternative network routing (local dialling)
  Note: I have received advice that all alternate routing for local calls could/should have been done before the 22 April. This is possible by including the new national and new local code together in the routing tables and this way no calls will be lost after the 22 April.
- International ISDN

Denial of Service Attacks - Yahoo / Amazon

By Deri Jones

Denial of Service attacks (DoS) occur commonly on the Internet, and about 20% of the >150 organisations security tested by NTA Monitor every quarter have significant exposure to such attacks.

Some Internet users make light of such attacks, on the basis that they 'only stop things working, they don't break into my site'. However, a Denial of Service attack can be part of a planned and focused attack, because:

- under certain situations when a system fails under the attack it may release information of real value to a hacker in it's 'last gasp' of life. Such information may be simply information on the directory structure of the internals of system, or worse still may be a 'core dump' information leak from which active accounts and passwords may be derivable.
- under a DoS attack, the victim site engineers may over-react to the problem, or may think it is a technical glitch not an attack, and may relax security systems in order to 'try to find out what's causing the problem'.

It's not unknown for sites to switch their firewall into 'allow all' mode for some minutes in a well-meant but misguided attempt to see if the firewall itself has a problem causing the loss of service.

Lastly of course, as in the case of the Yahoo incident, loss of service can be very damaging to a companies ability to continue to serve its customers, and may also lead to loss of credibility if the problems are not addressed quickly.

Attack methodology

How do DoS attacks like the Yahoo one work? Such attacks which depend on the production of very high traffic volumes, have a well known structure.

1. Attacker compromises many 'middle man' sites.
The attacker manages to take control of very many machines across the Internet - hundreds or more. This process may be fully manual or may be assisted with some attack tool software 'exploits'. Typically a rich source of machines that are easily taken over are universities... (there's a separate thread possible on what should be done about that!

2. Attacker installs distributed attack tool on them all:
A number of distributed attack tools such as Tribal Flood network (TFN), Trinoo and Stacheldraht (German for barbed-wire) have been in use recently. These tools when installed across many systems form a co-ordinated infrastructure for launching attacks - on the same model as a military General / Officer / squaddies basis. Or in spying metaphor, they allow a single attacker to control half a dozen or more 'controllers' each controlling maybe 50-100 'agents'.

3 The attack is launched:
The attack network can be started very quickly, and all agents can target a single victim with one attack, or may be grouped to attack a number of sites using different attack methods. In the case of Yahoo, the attacks involve triggering huge volumes of traffic - Gigabits/second of traffic - so were notable by their scale.

4 The victim responds:
Even a very sharp, attentive victim will have trouble responding to such a volume of traffic. the first step is to identify where the traffic is coming from (lots of places at once often), making a list of IP source addresses and then configuring the security perimeter to block all traffic from those addresses. However, the attack may be using fake IP From addresses - so blocking these will not actually stop the traffic at all. Secondly, if the attack agents are themselves bouncing their attacks through another middle layer of sites - ones which allow themselves to be used as 'amplifiers' of certain traffic types, e.g. Smurf amplifiers first reported in 1998 - then source of the traffic may be innocent organisations, some of whom may have legitimate traffic needs with the victim site so blocking their IP ranges will also kill correct traffic.

Lastly, even once the true source of the attack traffic is known and IP blocking is configured, this does not stop the traffic converging across the Internet and coming down the connection to the victim site - she's only managed to stop it going further by blocking at the perimeter. The victim's Internet connection is still overloaded and no normal traffic gets through.

The next step is to contact the ISP, and ask them to block the particular IP numbers at the ISP side of the victim's connection. This may take some co-ordination - how fast does your ISP jump?

The ISP themselves will also want to stop the traffic from coming *into* their network from outside (assuming it's not coming from customer networks within their own customer network), so the ISP has another round of blocking to implement, which may involve some tricky router changes. Furthermore the extra work load of checking FROM addresses on traffic (which normally an ISP's routers ignore totally, caring only about the TO address) may be too much for some of the ISP's routers if they are a little short on spare CPU capacity - so some blocking may not be possible. One ISP will then contact a neighbouring ISP for them to start blocking too, and it may be 4, 6 or 10 ISP's 'deep' before the actual source of the huge traffic volumes can be blocked at source - all the while the high traffic volumes across the Internet may well be slowing down genuine traffic, especially where particular links maybe short on spare capacity - such as often any expensive International leased lines.

There are however two types of DoS:

1. DoS vulnerability due to victim error / inadequate care

Many Internet sites have made an error in their security perimeter, or are running email, web or other software with known security bugs that make them vulnerable to a denial of service attack. Typically a server will crash under an attack that exploits the particular problem. Typically just a small amount of traffic is used in the attack, just enough to tickle the flaw.

Such attacks can be avoided for 99% of the time with proper security practise and keeping up to date with patches etc.

It is vital to have regular (quarterly or monthly) active security tests as part of this ongoing effort of maintaining the security bar.

2. DoS due to brute force

This flavour of attack does not depend on the victim having a security problem. The attack works by simply overloading systems at the victim site.

For example, one such DoS may involve bringing a web server down to a crawl and stopping legitimate users getting pages from it, by the brute force technique of requesting the same page so fast that it cannot keep up. This attack would simply need a normal web server at the victim site.

Grabbing web pages creates high volumes of outbound traffic (a small web page request may cause a 50K or more page to be delivered) and a high server load.

Grabbing SSL pages puts a higher 'load per page grabbed' on the server due to the extra load of processing the encryption elements of the SLL process.

The Yahoo attack, was also a brute force attack, but instead involved injecting high volumes of traffic *into* the site, by dint of having enough attack agents in parallel. It also used additional third party 'amplifiers' to multiply up the output of each individual agent. ('Smurf' amplifiers for example can produce hundreds of times more traffic targeted at the victim than the agent itself produces - allowing a modem (50Kb/s) connected agent to still saturate perhaps a 2Mb/s connected victim.

Wake Up call ?

Roy Hills of NTA Monitor (www.nta-monitor.com) said: "we often find and report potential DoS issues to our customers and sometimes also to their ISP when part of the ISP's infrastructure is found to be vulnerable. However, we find that this information is rarely acted upon because people don't take DoS attacks seriously.
Hopefully the recent high-profile incidents will act as a wake-up call by showing that these risks are real".

Conclusions

Denial of Service attacks will never go away - because the 'brute force traffic storm' trick will always offer an attack route.

Co-ordinated attacks like the Yahoo ones will continue and increase - and all high profile organisations are at risk. Maybe over the next couple of years if universities and other insecure organisations that are typically used by attackers to plant their agents will tighten up on security, and make it harder for the distributed attacks to plant enough agents. Expect some embarrassing high-profile media attention for UK Universities being used in major attacks in the next 6-12 months.

Non-Brute force DoS attacks can be reduced to virtually nothing by careful vigilance and regular ongoing active testing of an organisation's Internet firewall + perimeter systems. Penetration testing provides the best 'real world' picture of a site's security.

Co-ordination between ISP's is very patchy and will increase as it becomes more and more vital, for the stability of the ISP's themselves, for them to respond quickly to major brute force attacks like the Yahoo one. Organisations like LINX in London (www.linx.org) can play a key role in co-ordinating between ISP's.

More information: further resources can be found at:
www.nta-monitor.com/newrisks/jan2000/tfn.htm
www.nta-monitor.com/newrisks/feb2000/yahoo.htm

(live from 28/2/2000)

The Security Column

By John Hunter

I know that Y2k is long dead, despite attempts to keep interest going by reminding us of new important dates where systems could fail.

Unfortunately we all did so well, that it really seems to have become as interesting as watching paint dry. Unfortunately, in most cases the paint has dried. "So why are you bringing this up now?" you ask. Well, there seems to be one subject that people are not addressing - the 'quick-fixes' that were made that will eventually need to be properly sorted out.

I wasn't able to write my column last December, as I was in the Far East, leading a team trying to help a number of strategically important government departments ride the Y2k date change. In a timeframe covering days (less than 3 weeks - as I wanted to be home on Christmas Eve) the solutions were quite Draconian. Systems which were known would fail were switched off and manual alternatives (or at best standalone PC operations) were implemented. Networks were taken down, compliant servers re-deployed, mainframe data offloaded to PCs etc. Through all this, they were saved Y2k failure (according to my definition).

On a similar vein, I am reminded of a conversation last summer with an Access-based contract programmer working in a financial institution. He had been working with the in-house systems for years and had an enormous depth of knowledge about MS Y2k problems. He explained how he'd managed to get around these in some cases by programming in an assumption that two digit years larger than 30 should be considered as in the 1900's, and others taken as being in the 21st century. He didn't seem particularly concerned when I said that surely he was just moving the problem forward!

I wonder how much of the Y2k non-event around the world was the result of similar fixes.

The point of these examples is that I'm sure that there are still a lot of systems working in a 'temporary mode' with all their inherent control issues. Even worse, if many programmers followed my friend's route, there are now many systems which will suddenly fail, not at the clearly identified century date change, but at random times during the next few decades. Can I suggest that a post Y2k 'fix' audit be on your plan for this year? Please email me via Datawatch with your experience/stories.

IS Security is becoming more important daily, as we trade more and more in data, rather than physical assets. I have been intrigued at the recent activity following the release of a hacking program which enables a PC to read and copy DVD videos. If you are not in to the technology, you need to know that DVDs are coded to prevent copying. A rather clever guy wrote and openly circulated on the internet a program which bypasses this security.

The authorities, of course, attempted to deal with the problem and the copyright owners obtained an injunction through a judge in California for the hacker to stop circulating the program. It wasn't this which intrigued me, but the futility of such a move in the truly global internet community. Within hours of the injunction, I saw copies of the program, its source code, a description of the DVD encoding system and how it was circumvented on web sites around the world. Apparently there are many people who don't recognise the authority of a Californian judge in their country.

I know DVDs are a specific issue, but what if you substituted your own company's product into the above scenario? Has your organisation got a defence against international plagiarism like this?

What Qualifications?

By Adrian Simpson BSc ACA FIIA

There was a time in recruitment, as little as fifteen years ago, when computer auditors were not expected to be qualified.

Computer audit was still a relatively new discipline and practitioners could substantially be broken down into two categories. A small number of accounting qualified computer auditors who had gained their skills in external auditing and a larger number who had backgrounds in I.T. The I.T. industry continues to grow so rapidly and in such an unpredictable fashion that experience and the demonstrable ability to do a job has often been far more important than qualifications. Many computer auditors in the 1980's had previously left school with virtually no academic qualifications. Somewhere along the way they had discovered I.T., prospered and subsequently transferred into computer audit.

Unfortunately, the artisans of the past have increasingly fallen from favour in the computer audit recruitment market. Three factors have accounted for this.

Firstly, the educational system has expanded dramatically. Far fewer teenagers are leaving school without qualifications and in the last twenty years the number of new graduates per year has more than doubled. Academic qualifications are now far more widely held and whilst once it was considered a positive if you had them, it is now considered a negative that you do not. It is somewhat ironic that amongst older computer auditors I have met many with no qualifications who are demonstrably able, yet I have met a number of younger ones with qualifications, who are not. Qualifications do not necessarily translate into ability.

Secondly, whilst computer auditors with backgrounds in I.T. were once most common, this is no longer the case. Those with backgrounds in auditing who have developed computer audit skills are now most common. The archetypal young computer auditor is now a graduate who has spent two or three years with a top five accounting firm in risk management or was an internal auditor, probably accounting or MIIA qualified, who has been given the opportunity to transfer into computer audit.

Lastly, computer auditing in the guise of the CISA or QiCA qualification now has its own established professional qualifications. It is worth pointing out that in purely recruitment terms, these two qualifications are essentially interchangeable. It does not matter which one you hold. The amount of study and preparation needed to acquire either of these is relatively small when compared to an accounting qualification or an MBA. However, because they exist, they are becoming de rigueur. I certainly now see job descriptions where the CISA or QiCA qualification is no longer confined to the "desirable" column of requirements.

The message now is that if you are going to compete in the recruitment market you are going to need more than just experience to sell yourself.

Some advice? Whatever qualifications you decide to undertake do them as early and as quickly as possible. The earlier in your career you complete a qualification, the longer you will have to benefit from it. If you leave it too late, the costs of acquiring the qualification in terms of time and expense generally outweigh possible financial or other career benefits.

Choose a qualification that you are going to complete. In recruitment terms starting a qualification and failing to complete it is worse than useless. Viewed in a critical light, people fail to complete professional qualifications for one of two reasons, lack of ability or commitment - neither of which are particularly complimentary.

Decide how much time you have available and are prepared to devote to a qualification. For example, if you are not a graduate and you decide to complete a part time degree, make sure that you are going to be able to study over a three or four year period. It is not a bad idea to go for a final qualification that has intermediate levels. For example the ultimate MSc you are aiming for may have intermediate diploma and degree stages where you can call a halt and have a perfectly legitimate qualification. Time spent investigating a qualification before embarking on a course of study is rarely time wasted.

If you have already embarked on a career and are a few years into it, it is unlikely that giving up work to study full time will ever provide a return that will make the original investment worthwhile. For example, do not loose a year's salary and spend many thousands of pounds completing an MBA in the expectation that your career prospects as a computer auditor will be transformed, they will not.

Professional qualifications have more value in the recruitment market than academic qualifications and we are rapidly approaching a time when the vast majority of employers will expect their computer auditors to be qualified. For anyone reading this who is not qualified and is at some time in the future planning to become active in the recruitment market, I would invest what is the relatively modest amount of time and expense in acquiring the CISA qualification. The sooner you do it the better.

Whither CISA?

By Derek Oliver, CISA

The first duty of ISACA's Certification Board is to maintain the quality and international reputation of our, highly respected CISA qualification.

Not only do we "set" the annual examination, using questions extracted from the Item Pool in the correct proportions according to the current domain structure, but we have the final vetting of all questions passed by the Test Enhancement Committee (TEC) before they are accepted into that pool.

It is our main duty to ensure that CISA continues to reflect the IS Audit profession. To this end, we periodically arrange for a survey of CISA's to establish to what extent the domains, and tasks within those domains, represent the overall, day to day work across several continents, and many cultures. Such a project is currently underway and some of you will have received questionnaires: On January 31, 2000, the CISA Job Analysis surveys were distributed via postal mail to 1,000 CISA's who were randomly selected from the central database. These individuals were also e-mailed an invitation letter informing them that they would soon receive the survey through the post. The Certification Department at ISACA Headquarters are in the process of putting the survey on the ISACA web site for on-line completion. Once this is successfully completed, they will select an additional 1,000 CISA's and email them a letter introducing the Web-based survey and all the information needed to access it.

So, to some extent, this article is by way of an appeal to those of you who have received, or receive in the future, such an invitation. Please, please do respond as we really do need your feedback to make sure we're getting near to the target, if not actually meeting the needs of everybody.

So, that's where CISA is going; I would expect to find a new set of "domains" emerging from the study, with different emphasis. Perhaps more stress on the importance of understanding the "business" ? No doubt more highlighting of business continuity, perhaps as a separate domain ? The exercise must be completed very soon as we're meeting in Chicago at the end of April to go through the whole pool of questions. We must re-allocate each one within the final domain and task structure - a massive exercise in itself - and by the end of August, we will be meeting to agree the 2001 exam, which will be based on that new structure; a truly representative qualification.

Other Designations, Certifications, Qualifications and Status.

A part of our "brief" is to maintain close relations with other certifying organisations, such as the IIA, Chartered and Certified Accounting bodies in various countries etc. We look at what they are offering and how CISA can dovetail with their needs, which is why the IIA now offer CISA's exemption from paper 4 of the Certified Internal Auditor (CIA) examination and the IIA-UK offer exemption from the first year of the two-year Qualification in Computer Auditing (QiCA) programme. We are talking with the Canadian Institute of Chartered Accountants and other, similar organisations about close working relations in the criteria of their qualifications.

The Certification Board also has to perform as arbitrators whenever a CISA appeals against revocation of his or her certification. This can happen for failure to pay the annual dues or not complying with the CISA/ISACA Code of Practice but, most often, is for failure to meet the CPE requirements. This is a relatively minor, though most important aspect of the Board which has resulted in, for example, to the founding of "Retired CISA" status.

Whither Certification?

But what of certification within ISACA ? We are, after all, the "Certification Board", not just the CISA Board and we have set ourselves some medium-to-long-term objectives to look at other areas where ISACA might be able to offer certification. Obviously, with the massive amount of work we're doing on the Job Analysis Study, such matters are still in their infancy but we have discussed the potential for :

- a "Son of CISA", i.e. a more advanced CISA designation, perhaps more involved in management and business issues
- a technically based certification; especially relating to control and security professionals rather than IS auditors
- a certification in IT Governance. As you know, ISACA has founded the IT Governance Institute to promote and develop the concept amongst both IT and business management
- a certification of competence in using CobiT in business management and/or auditing

Well, that's the plan. There's a lot of hard work yet do be done, but we are living in exciting times ! If you, as an ISACA member, have any ideas just let me know. They will be thankfully received and faithfully applied to a future Board meeting.

Central News

By Michael Hughes, President, Central UK Chapter

Well it looks as though we all survived the changeover to the new millennium.

However, it now seems that for some organisations, the inquisition has started into whether the investment in time and capital spending really was necessary.

Well, what would have happened if we hadn't taken appropriate action and ignored the issue? A major benefit coming out of the Year 2000 issue, has been the raised profile of IT, bringing it to the 'top table' and demanding senior management awareness of how pervasive and valuable an asset IT really is.

Now that we can finally put the Year 2000 behind us, what is the next challenge for us information risk professionals? Well, that's easy to answer, it is the e-revolution. Why is this such an issue, the message is quite clear and can be summarised by the following key points:

- e-business is impacting organisations across the board, regardless of their area of activity and regardless of their structure;
- the use of the internet is not a technology issue, it is about reengineering the organisation;
- speed and flexibility are essential for success in e-business;
- it's not a one-off inititive, evolution will be the key;
- if you don't, your competitors will;
- traditional market barriers are crumbling;
- the changes are inevitable, they are happening now;
- organisations ignore the developments in e-business at their peril.

You all need to be aware of these changes and you should be actively thinking how they are likely to affect your organisation and where you should have a proactive involvement to identify risk and to recommend measures to effectively mange this risk.

A key issue with e-business is ensuring that technology is fully exploited to gain business advantage. This presents new risks for organisations and it is important that in the rush for new technology risks and controls are fully considered.

Why are companies carrying out e-business?

Basic drivers for e-business are revenue growth and cost reduction. E-business has the potential to change the way in which we buy, sell, bill, make payments and market products. In other words, a fundamental change to the way in which organisations do business. There are tremendous opportunities but with them come new threats.

A classic and often quoted example is of Amazon.com and book retailing in the US. Until a few years ago there was little threat to established book retailers, with large capital investment required to set up a book store chain. In only a few years Amazon has grown rapidly and now rivals Barnes and Noble, previously the largest book retailer in the US. This brings home the message that e-commerce is a business rather than a technology issue.

Christmas 1999 was seen as being the first e-Christmas. Initial observations seem to show that online retailers have suffered a number of issues that could in the short term damage their brands and cause customers to switch on to competitors. These can be summarised as:

- underestimating the necessary physical infrastructure to distribute products within a tight timeframe;
- underestimating the demand for products and services being offered, resulting in consumers being unable to access web-sites or order sufficient quantity of goods;
- not having fully tested solutions in place leading to problems such as incorrect pricing, orders not being taken correctly and orders being missed from shipping lists.

The competitive environment for organisations has also changed and become much more dynamic. Companies can now face competition from firms, potentially from across the world. On a business to business level, customers are now starting to demand the use of internet enabled supply chains.

Despite the current press emphasis on business to consumer e-commerce the real value lies in

business to business electronic trade. E-procurement allows procurement processes to be changed significantly and reduce the amount of time and paperwork associated with individual purchase orders. However, successful e-procurement is dependent on underlying IT infrastructure and an effective management information system.

Key e-business risks

There are a number of key risk areas that could be affected by the introduction of e-business to an organisation:

✦ Strategy - Has the organisation thought clearly about their business strategy and the business advantages and implications of electronic commerce.

✦ Business processes - In order to provide an acceptable level of service, e-commerce activities will have to be incorporated and integrated with existing business processes. This includes the potential sudden expansion into a global market.

✦ Reputation - A key factor for organisations is the potential damage that trading on the Internet could cause to business reputation. Senior management within the organisation needs to be aware of the potential pitfalls of e-business. Web based business is dependent on IT and any IT failure will have an immediate and direct effect on the ability of the organisation to trade and on its reputation.

✦ Security - e-business increases the potential for IT security breaches. Transaction may take place on-line and a secure Internet environment is key to the business reputation and effectiveness of an organisation.

✦ IT capacity - Selling over the web and web based links with trading partners present new challenges from an IT perspective. IT systems have to be available 24x7 with appropriate support.

✦ Legal and regulatory - this is a developing issue. Governments are trying to understand how the new medium of e-business fits within the existing legal framework, both nationally and internationally. Organisations involved in or planning to become involved in e-commerce are potentially exposing themselves to a multitude of new legal issues and potential legal risks. Key areas of uncertainty are the formation and existence of online contracts, breaches of copyright and trade mark issues, data protection issues, taxation, negligence conflicts of laws, breaches of laws in foreign jurisdictions where new markets are being accessed and the financial services regulatory regime.

✦ Third party reliance - the infrastructure and nature of the Internet mean that organisations will need to rely on a variety of third parties, or require new and additional services from existing third parties such as ISPs, telecommunications providers and external IT supplier.

✦ Monitoring - web based commerce will be open to the global market 24 hours per day. In view of the potential reputational damage which can be caused to the organisation, it is key to ensure that web based trading links are closely monitored.

Most of the areas discussed above require controls and checks to be designed into the systems and processes, to effectively manage new technologies and methods of doing business over the web. Therefore, as risk professionals, we need to be involved in e-business initiatives from the start, and throughout the project, ensuring that senior management have appropriately considered these key issues.

As an example of this, we were recently involved with a retailer facing increasing online competition, who was in the process of setting up an e-commerce website. Following our initial review, we discovered that although they had employed a web developer to set-up a website, the organisation did not have appropriate mechanisms in place to fulfil and sustain customer orders made online. The launch of the website was put on hold until we had helped the retailer address the underlying business and systems issues of e-commerce.

We all have a vital role to play to help ensure that our organisations fully exploit the use of this technology whilst effectively managing risk.

Central Chapter Programme of Events

30 March 2000 - Gary Hardy
Cobit III

April 2000
Post Millennium Blues Dinner

25 May 2000
AGM/Penetration Testing

14 July 2000
End User Computing

22 September 2000
Business Continuity Planning

We extend a warm invitation to ISACA members of other chapters who find themselves in the area and would like to come along to any of the meetings

Northern Chapter Programme of Events

22 March 2000
CAATs Conference
Salford

19 April 2000
COBIT (As audit tool)
Bradford

May 2000
Internet - Control issues and Audit Methods
2 day seminar
Salford

28 June 2000
AGM and Running a Computer Crime Unit
Chester

NEWSROUND

By "The Newshound"

TFN for DOS

As E-commerce gets set for explosive growth, the magnitude of so called 'denial-of service attacks' also looks set to increase.

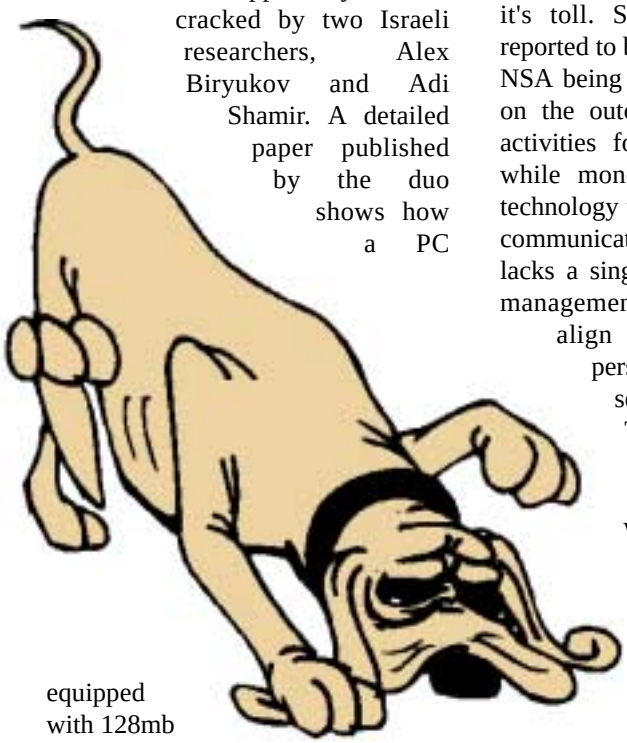
A new set of hacker tools called Trin00 and TFN , first detected in August 1999 are now being traded in the hacker community. The packages were revised in December 1999 to more advanced versions with improved functionality.

The tools enable a hacker to co-ordinate a Web site attack by enlisting the help of thousands of unwitting 'slave' computers to cripple a site. They are solely destructive and targeted at large commercial or public sector systems running UNIX.

The TFN package consists of two programs. Firstly a server talks to multiple clients using a broken version of the 'ping' protocol. Instead of sending icmp echo request/replies, it sends only icmp echo replies. The theory behind this is that many sites permit icmp echo reply through their routers, as it is convenient to be able to 'ping' out into the world. Commands can be issued to tell a client to start sending large numbers of packets to the selected victim. The server is designed to co-ordinate the launch of attacks between various disparate remotes, flooding the victim with meaningless traffic. The Trin00, ('Trinoo') package performs a similar function but uses UDP highports, (31335 by default), for the 'master' to communicate to the 'bcasts'.

GSM Cracked

The New Year also bought some news from Tel Aviv. The encryption scheme protecting the global system for mobile communications, (GSM) has apparently been cracked by two Israeli researchers, Alex Biryukov and Adi Shamir. A detailed paper published by the duo shows how a PC equipped with 128mb of RAM and a substantial hard drive can penetrate the 'A5/1' encryption method and decipher a GSM transmission in less than a second.



There are over 230million users of GSM mobile phones worldwide who account for 65% of the total market. Some mobile 'phone companies remain sceptical but David Wagner, a computer researcher at Berkley has validated the claims and now believes that GSM communications are wide open to corporate espionage. So next time you are on the company mobile be careful what you say.

Spooks are out of Control

Now spare a thought for the beleaguered NSA. The rapid pace of technological change is apparently swamping America's premier security agency. Despite having the largest pool of the most advanced supercomputers in existence, the strain of breaking every newly released encryption algorithm, intercepting messages on fibre optic cable, eavesdropping on email and the sheer scale of trying to monitor the explosive global growth electronic communications is taking it's toll. Systems development is reported to be 'out of control' with the NSA being accused of lacking focus on the outcomes of its monitoring activities for the nation. Crucially, while money is being thrown on technology to stay ahead of the latest communication advances, the NSA lacks a single corporate information management system to track and align budgets, missions and personnel so that it can make sense of what it is doing. The situation has got so bad that US Air force Lt Gen Michael Hayden, who, at the time of writing, has headed the NSA for ten months is calling for '100 days of change' to reassess the corporate direction and objectives of the agency and try to bring expenditure back under control.

Big Brother is an Aussie

Australia's new Security Intelligence Organisation Legislation, passed at the tail end of last year, appears to set a precedent in the English speaking

world. The new law enables the Australian Security Intelligence Organisation, (the 'Aussie' equivalent of the CIA or MI5), not only to monitor private computers throughout the continent but change any data they may contain. Under the legislation the Australian attorney general can authorise legal hacking into any computer system including the copying and alteration of data as long as he has reasonable cause to believe that it is in the interests of 'security'. The new law places some restrictions on the introduction of computer viruses or interfering with data used for lawful purposes. However even this protection may be overridden if the selected course of action can be shown to be 'reasonably incidental' to the investigation.

There are genuine fears that the new law may hamper the growth of antipodean e-commerce as the law would permit encryption keys to be legally lifted from private computers almost at will.

SAP Hole

And now something for all you SAP users, the Technology Evaluation Centre has uncovered a potential security hole in SAP R/3's three-tier architecture. SAP expects the database or third party products to handle security between the application server and the database server. If the client elects not to take these extra measures, the master password for the SAP database travels over the network in clear and can be captured. Apparently PeopleSoft, a SAP rival in the ERP market has the same problem. To be precise, Dr Peter Barth, Technology Marketing Manager for SAP AG in Walldorf Germany, gave this response in answer to TEC's question on the issue.

> "*SAP supports for the connection between database and application server support by security standards provided by the database as well as open interfaces to external security products. Typically, database specific features from e.g. Oracle, MS SQL etc - are used to protect initial logon. In case the data transfer needs to be secure, also either database specific or database independent security mechanisms can be used. However, note that SAP advises to use a separate internal subnet in the networking environment. Thus, it is physically impossible to sniff, the security mechanisms are not mandatory. Note that the application server and database server are expected to be in a LAN environment and not connected via WAN or open Internet connection to the outside world, (only the presentation client should be used over WAN and open Internet connections: here security can be achieved by various means (e.g., PKI infrastructure)."*

So next time you do a SAP audit maybe you should ask some pertinent questions!

Burnt Cookies

The cookie men on the Internet could be in for a hard time. A new service from Zero Knowledge Systems based in Montreal has developed software to allow people to remain completely anonymous and untraceable when they surf the Web. Zero knowledge says that the software was developed to address a growing concern among net users that Internet companies are deploying technologies which allow them to become evermore intrusive in tracking the buying habits, age, interests and home addresses of net surfers before barraging them with electronic 'junk mail'. Using the software enables a surfer to cruise the Net without leaving any trace of their browsing habits. The software works by identifying only the final portion of the computer network used to transmit the information. It also allows up to five pseudonyms to be used for email addressing. Trial software is available from the web site at www.freedom.net but hurry as the company is limiting it to the first 10,000 users.

Stormy Weather for Satellites

Just when you thought Y2K was over and it was safe to venture over to the developers desks again Reuters have released of further disruption likely to take place in 2003. This is all down to the Sun, (no note Ruperts daily comic - the big yellow thing in the sky). The Sun goes through an 11 year cycle of pulsating in an out, (a bit like a failed weight watcher). When it next bursts its seams in 2003 at what is called the 'Solar Maximum' it discharges huge volumes of ionised particles in the general direction of the Earth. This can result in damage to communication satellites, radio transmission problems and electrical disruption. During the last Solar Maximum in 1989 the entire province of Quebec in Canada was plunged into the dark because a geomagnetic storm caused the power lines to overload.

IR Computer Glitches to Blame for Inaccurate Assessments

The Inland Revenue has suffered embarrassment in a survey conducted last year by the Association of Chartered Accountants. The survey revealed that 96% of taxation self-assessments were inaccurate to problems with the IR software. At the time EDS, which runs the IR computer systems, scoffed at the claims although a spokesperson has admitted that there was problem but on a much smaller scale.

In March this year EDS launched its own investigation following the discovery that 20,000 people who filed tax returns on time were 'accidentally fined' £100.

EDS claims that these were all due to human error and had nothing to do with the software. The ACCA's new survey is due to be released in March. It could make interesting reading.

10 Years Ago

By John Hunter

Back in 1990, Electronic Data Interchange (EDI) was all the buzz.

Thomas Carver of the then Coopers & Lybrand Deloitte, gave Datawatch an explanation of this technology for the transmission of business documents in a standard format between companies. It was a yet another brilliant conception, which, despite having been around for a number of years, still couldn't quite reach the mass market.

"Today, approximately 5000 companies in 50 industries world-wide are using EDI to some extent. The benefits resulting from the use of EDI include reduced processing costs and more efficient business operations. EDI lowers processing expenses by reducing manual data entry, paper and mailing costs, and error correction. In addition, EDI can improve customer relations, production scheduling, cash management, and inventory management.

The most common technique used to transmit electronic documents from one company's computer to another's involves the use of an independent third-party network, which acts as an 'electronic mailbox' between EDI partners. Direct links between computer systems also exist, but are not as widely used due to the complexities involved in establishing direct links with multiple trading partners."

He then went on to describe some of the control issues….

"Exchanging data using EDI introduces financial and operational control considerations inherent in the electronic environment. Because EDI replaces paper documents with electronic ones, new control techniques need to be developed and implemented. Typically, these include both manual and automated techniques, and can affect an organisation's existing internal control procedures.

Control techniques are required throughout each function performed during EDI, as the data is transmitted, translated, and passed to the application system - all via electronic means. The audit trail for the transactions will have to be modified to take into account the electronic paperless environment.

At the transaction level, controls need to be designed and implemented that address the completeness, accuracy, and authorisation of EDI-transmitted data. Once the data is in the application system, it is subject to controls that apply to all data processing by that system.

EDI may also impact control procedures within the data processing operation, or information technology (IT) controls. When EDI programs are developed, maintained, secured and operated using the same processes as regular application programs, there generally is little effect on the control procedures that already exist within those same processes. However, because of the unique characteristics of EDI, new issues are raised in each of these processes and should be addressed by the organisation. In addition, if EDI is implemented and maintained by a group outside of data processing, the same controls that exist within the MIS organisation need to be established over that separate EDI environment."

He raised a number of operational control issues exposed by EDI processing, including:

- Do electronic transactions require a separate legal framework?
- Is an electronic document a valid contract without a signature or without being written in the traditional form?
- What constitutes a valid signature?
- Since EDI transaction files are the only source documents, how long should they be retained?

With EDI advancing and becoming more prevalent, users and auditors are now focusing their attention on financial and operational control issues. Auditors are facing issues related to the timing and recognition of financial transactions and the storage, retrieval, and review of documentation. Information technology (IT) controls, such as the security of the EDI transactions, are being assessed. In some advanced EDI environments, invoices are no longer required to trigger payment, as there is only a match between the purchase order and the receiving records. Legal agreements and the enforcement of contracts are also key issues."

I think that we are getting close now….

Answers to Linkages on page 2 ...

1. Teeth
2. User
3. Get
4. Old
5. Net
6. Under
7. Car
8. Sand
9. Rat
10. Outer
11. Inch

The initial letters of these answers form the word "Outsourcing"