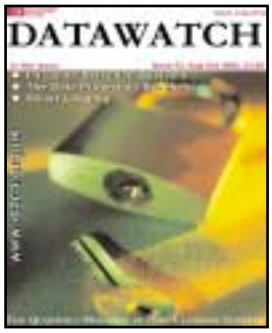
53, Aug-Oct 2002

DATAWATCH



Information Systems Audit and Control Association

DATAWATCH is published by the ISACA London Chapter. Membership of the chapter entitles one to receive an annual subscription to DATAWATCH.

Opinions expressed in DATAWATCH represent the views of the authors. They may differ from policies and official statements of the ISACA London Chapter and its board, and from opinions endorsed by authors' employers, or the editorial team of this magazine. ISACA London Chapter does not attest to the originality of the authors' content.

10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE26 1SD
www.isaca.org.uk
nancy@isaca.org.uk

In this issue:

regulars

ISACA London Chapter Committee 2002/2003

PRESIDENT
Charles Mansour
01322-223714
cmanso@globalnet.co.uk

V.P./WEBMASTER
Allan Boardman
Goldman Sachs
07881 930914
allan@internetworking4u.co.uk

TREASURER
Archie Watt
BDO Stoy Hayward
020 7893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Joseph Wright
HSBC Holdings PLC
020 7260 6843
Joewright@HSBC.com

PAST PRESIDENT
John Mitchell
LHS Business Control
01707 851454
john@lhscontrol.com

PUBLICATIONS
John Hunter
HLB Development Consulting
01635 248944
jhunter@hlbdc.com

PUBLICATIONS
Paul Fortmann
07788 413996
paul.fortmann@btinternet.com

PUBLICATIONS/RESEARCH
Kamal Khan
Rabobank International
020 7809 3935
khank@rabo-bank.com

CISA CO-ORDINATOR
Michael Christodoulides
District Audit
01438 351570
m-christodoulides@district-audit.gov.uk

MEMBERSHIP
Terry Fallon
01189 473511
Terry.Fallon@talk21.com

EVENTS
Nick Fellows
Barclays Bank plc
07775 543153
nick.fellows@barclays.co.uk

EVENTS
Peter Andrews
PJA Consulting Ltd
020 8540-0224
pa@pjaconsulting.co.uk

EVENTS
Mark Hughes
London City Audit Consortium
020 8836 5899
mark.hughes@bartsandthelondon.nhs.uk

GENERAL
Christine Maxwell
KPMG
020 7311 2327
christine.maxwell@kpmg.co.u

GENERAL
KevinHandscombe
KPMG
020 7694 6083
kevin.handscombe@kpmg.co.u

CHAPTER OFFICE
Nancy Watt
01487 815705
nancy@isaca.org.uk

ISACA Northern UK Committee (officers only)

PRESIDENT
Ray Butler
HM Customs & Excise
0161 827 0875
ray.butler@hmce.gov.uk

VICE PRESIDENT
Robert Newbould
Corus plc
Bob.Newbould@corusgroup.com

TREASURER
Ian Simpson
Halifax plc
IanDSimpson@halifax.co.uk

SECRETARY
Peter Thompson
Deloitte & Touche
peter.thompson@deloitte.co.uk

MEMBERSHIP
Alan Rainford
Axa Insurance
01253 662782
alan.rainford@axa-insurance.co.uk

CISA CO-ORDINATOR
Gan Subramaniam
Homeloan Management Ltd
01756 692147
gsubramaniam@skipton.co.uk

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

WEBMASTER
Peter McCready
MBNA Europe Bank
01244 67200
www.isaca.org.uk/northern

ISACA Central UK Committee (officers only)

PRESIDENT
Mike Hughes
KPMG
0121 232 3207

VICE PRESIDENT/CISA
Simon Parker
Capital One
0115 843 6456

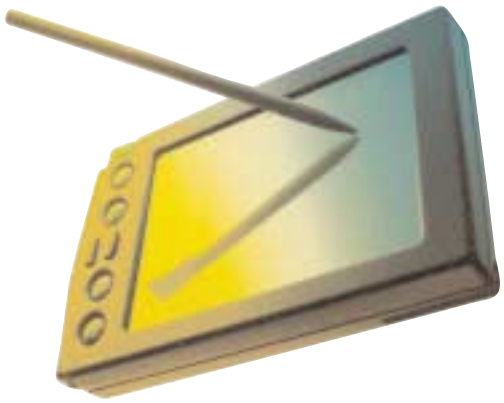
SECRETARY
Chris Chandler
Arthur Andersen
0121 233 2101

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:

www.isaca.org.uk/central



Well, this is my last Datawatch (sniff) and the last of my contributions to Netwatch. How am I going to cope?

I am handing the editorial reins over to Paul Fortmann, one of our many new committee members. Netwatch is being handed over to Allan Boardman who is also the Web Site Manager for the London Chapter.

The Publications Team also welcome Kamal Khan who has side-stepped from Membership. We've managed to hold onto John Hunter and Nancy Watt, but say goodbye to Bill Hawkins.

Back to business - another interesting range of articles this issue. Mark Osborne of KPMG asks the question "IDS - Are they catching hackers or just script-kiddies?". The Data Protection Minefield is covered by Derek Oliver and Neil Jarvis talks about Smart Logging.

There are of course our regulars, Security Column, Netwatch, Career Column and From the Bulletin Boards. There is also an update on the Research Board activities that you may find interesting.

You'll also find (below) the London Chapter Events planned for this coming season and details of the CISA training that we are offering for 2003.

So, it just remains for me to say goodbye and good luck to the new Publications Team and make sure you check out the next edition of Datawatch for a new, fresh looking Netwatch!

Happy surfing!

London Chapter Events 2002/2003

INTERMEDIATE - AUDIT	**26 September 2002** Information Governance (FSA, N2 & The IT Auditor) Vernon Poole KPMG 20 Farringdon St	INTERMEDIATE - AUDIT/SECURITY	**24 October 2002** Implementing IT Governance Paul Williams KPMG Salisbury Sq	ADVANCED - AUDIT/SECURITY	**28 November 2002** Risk Management in 2003 Gareth Rowland ABN-Amro 250 Bishopsgate
INTERMEDIATE - AUDIT/SECURITY	**19 December 2002** Internet Threats & IDS Kenneth de Speigeleier ABN-Amro 250 Bishopsgate	INTERMEDIATE - AUDIT/FORENSICS	**23 January 2003** Spreadsheet Fraud Ray Butler Venue to be confirmed		
ALL LEVELS - AUDIT/SECURITY	**27 February 2003** Information Security Speaker to be confirmed ABN-Amro 250 Bishopsgate	INTERMEDIATE - AUDIT/SECURITY	**27 March 2003** Control Over Internal & External Outsourcing Charles Mansour ABN-Amro 250 Bishopsgate	ADVANCED - AUDIT/SECURITY	**24 April 2003** CRSA & the IT Auditor John Mitchell ABN-Amro 250 Bishopsgate
ADVANCED - AUDIT/SECURITY	**22 May 2003** Data Protection - What's Coming Up & Implications For Systems (& AGM) Stewart Dresner ABN-Amro 250 Bishopsgate	INTERMEDIATE - AUDIT/SECURITY	**26 June 2003** E-Risk Revisited Speaker to be confirmed ABN-Amro 250 Bishopsgate		

I'd like to say (in the words of my fellow Scouser, Ken Dodd), how tickled I am to be selected to be the London Chapter President for the coming year in place of my good friend Karen Sharpe..

I'll be in the post until next May. I have a pretty powerful team behind me in the form of the Chapter Board and our Chapter Administrator Nancy Watt. I'm sure you'll see the benefits flowing through in the coming year.

To be really successful, we need to be good at delighting our customers (to use the 'in' marketing phrase). Our customer is you, a London Chapter member. To get to the delightful state, we need to understand what it is our customers want. And that's where it gets a bit tricky, as the IT Audit and Control community seem to be a pretty taciturn bunch of people. We do get some limited feedback from the members as to what they want, but by and large, your Board is left to 'second guess' membership needs and concerns in the absence of direct customer input. This does make it a bit difficult to gauge what our customers (you) want and what they're feeling about life, the (audit) universe and things in general.

In addition to the things we do really well as a Chapter (e.g. Datawatch, CISA Review Courses, our WEB site, and our monthly technical presentations, to name but a few) we feel we can deliver even better membership benefits. It seemed to us that one way to do that was to provide quality IT Audit Training workshops at reduced cost (we don't need to make anywhere near the margin that our value added training colleagues make). However, last year there turned out to be little in the way of take up and all the events that we planned had to be withdrawn. We'll be going back to the drawing board to see if we can do it better this year. It'll help our Events Committee greatly if we know what the current needs are.

Where you can make a difference is to let us know exactly how you'd like to see things developing over the next year. It's not just about events! What are your needs as a member of the London Chapter? What do you feel are the constraints that prevent you getting the maximum value from your membership and where do you think we could improve?

It's never been easier to communicate!. You don't even have to bother with a stamp and envelope. Just get your virtual pen and paper out and let us know. E-mail your thoughts to me or to any Board Member. The Board will be interested to get your thoughts and ideas. Even better, get along to the monthly meeting and 'buttonhole' your Board Members.

We want to see you delighted in a year's time!

Security Audit and Control Features SAP R/3 A Technical and Risk Management Reference Guide

This guide has been designed as an education resource for control professionals. It is the stated intention of this book to enable auditors, risk and security professionals to evaluate the risks associated with SAP R/3 and design appropriate controls to manage such risks. The book is designed to be a practical "how to guide".

In reality the book will appeal to a wide range of readers. The Introduction to SAP R/3, Strategic Risk Management and the sections related to the individual SAP modules are excellent for business and audit managers whorequire an overview which is factually authoritive and memorable.

Ironically, the all encompassing nature of enterprise resource planning systems such as SAP R/3 also makes this an ideal reference guide for individuals who are beginning their IT audit career. The book clearly describes the technical and business regime in which SAP R/3 is found, has cross references to ISACA's COBIT tool and includes detailed audit programs in a professional presented and easy to read package.

The Information Systems and Controls Foundation bring together experts in the field information system and control and SAP R/3. This book has greatly benefited from the input of a broad range of technical and management experts.

Over a very short period of time I have found that this guide has become my preferred first choice of enquiry when seeking an answer to a management or technical query related to the control of SAP R/3.

Michael Christodoulides, CISA, is an Information systems auditor currently specializing in local government and health sectors. He has over 8 years information systems audit experience in private and public enterprises. Michael is a Board Member of the London Chapter of ISACA. The full review will appear in volume 6 of the Control Journal.

En-light-en-ed (en līt/ən ed), v. **1.** having received intellectual light. **2.** having light shed upon **3.** having seen the brilliance of a good idea: *having registered to attend the* 31st International Conference *presented by* **Information Systems Audit and Control Association®**

international CONFERENCE

31st Annual International Conference and Annual General Meeting of the Membership

The world's leading conference for IT governance, control, security and assurance

20-23 July 2003
Singapore

Presented by Information Systems Audit and Control Association (ISACA™)

Earn up to 33 CPE Hours

www.isaca.org

IDS - Are they catching hackers or just script-kiddies??

Mark Osborne, KPMG

Instead of moaning about it, why don't you do something about it? snapped one of my Penetration testers, as he sprinted out of the office with a handful of bizarrely configured Linux laptops. The conflict, as ever, had been born out of good intentions. He and his team of nearly house broken pentesters, of which I had been a founding member (before hair loss followed by a related credibility loss forced me to re-specialise), had broken into another organisation. That should be good news. Unfortunately, the client had spent lots of money on an Intrusion Detection System (IDS) which had dutifully alerted them to every attack we launched, excepted the one that actually worked and got us in. The manager at our client was furious - with us, which was a real case of shooting the messenger.

In an effort to placate both client and my long suffering team, I have written this article to highlight some of the more common problems in Intrusion Detection - which will be soon be acknowledged as essential technology just like Virus Scanners and Firewalls.

What is an Intrusion Detection System?

An Intrusion Detection System (IDS) is effectively the computer equivalent of a burglar alarm. Their main purpose is to provide warning of when a hacker breaches your security regime and accesses your IT system. They come in a number of different varieties but can be usually divided into two. Host-based IDS (HIDS), where software agents are installed on your key servers, then watch for computer misuse and break-ins. The other major type is the more popular and easier to deploy, Network-based IDS (NIDS). These are positioned at key points of the network inspecting passing traffic for signs of computer misuse and break-ins.

Perhaps of greater interest to those who didn't know this is that IDS is one of the latest trendy subjects in IT security. And despite the fact that it is not a new technology, there are plenty of snake-oil sales men about who will tell you it's a plug and play solution to end all your worries. Even as a great fan of the kit, I wouldn't promise that.

There are many areas within the IDS arena worthy of discussion:

Security Strategy and architecture - most of us work in a commercial organisation that has specific objectives that are sometimes translated for us into project objectives. These objectives are often not as informed as they could be - take it from me a hardened consultant, when times aren't tuff, executives are often delighted to spend thousands to make that nasty internal audit report or regulator leave them be (some Financial sector regulators specifically require IDS deployment). But if events result in deploying IDS and it cures the original problem, we regularly find it does not complement the overall security architecture of the organisation or that the budget stops other potentially more important projects taking place (stronger doors often provide better security than louder alarm bells).

But this isn't a woolly area like so many that can oft be associated with Security Strategy/architecture (I read a paper on Security architecture from a much respected forum which include some of my much respected mates stating that "we agree it isn't all techie and we agree it isn't all standards but we can't agree what a Security architecture is"). This area can have a huge bearing on the overall safety of your data and will include discussions on:

1. What deployment strategy will you have - Perimeter only, Perimeter and hi-risk zones or full internal?
2. Who should maintain the architecture and what organisational changes will need to be made to enhance and align the whole regime?
3. What IDS type should be used?.

Reaction - By far the biggest problems I have experienced in the last ten years dealing with Internet security have been in the area of incident response. By far the simplest question you should ask yourselves is "Are you ready for the machine when it goes beep?" because if you're not why have you bought an IDS in the first place. Knowledge of your own exposure will only have a most disquieting effect on the management.

This is a fantastically exciting and interesting area covering;

- The aligning of your detection policy to match your incident response, especially insuring that when the machine goes beep there is someone there to hear it.
- Establishing incident response procedures to ensure that the appropriate permissions/authorities are obtained from senior management, and that links with other departments like PR, HR, IA and Legal are established.
- Formalising the setting up of your internal CERT with all that includes on the organisation front

Implementation of NIDS - The common problems found in the design and implementation of IDS.

All of these categories are worthy of an article in their own right but for this article I have chosen the latter, with a strong focus on NIDS because they are more common and more problematic.

Problems with NIDS

There are three main areas where IDS can have problems:

- Inferior IDS - Device misses attacks that it should pick-up
- Poor deployment
- Poor configuration

Each of these will be dealt with in turn.

Inferior IDS - Device misses attacks that it should pick-up

The first NIDS, I encountered was Courtney. At the time, SATAN ruled the earth - that was back in the dim distant time before E-commerce or at least, before money was made on the Internet. Also at the time, many IT security staff didn't know much about computers - it was all policy documents and passwords. So when SATAN (the scanner not the dark one) came along and provided a set of intrusive analysis tools that could be run from a GUI by

novice, as an alternative to forcing you to write "c" code and run strobe from the command-line, the world was rocked. CERT advisories were issued about SATAN and many panicked.

Courtney was born-out of this. It was a little *perl* script that read *tcpdump* output and sent out messages if a series of connection were detected within a set period - it was very effective. But the code was published and so people soon found ways of avoiding it detecting their probes. And that is really what this section is about - hackers call it IDS avoidance.

When deploying or choosing an IDS you have to be aware of the common faults in the technology and the way they can be exploited or avoided. This will help you purchase a device which best suits your needs, or allow you to minimise the effect of any less-than-perfect features of the technology used.

Dropped packets

NIDS are particularly susceptible to performance problems since one sensor device has to receive, interpret and react to network traffic created by many (many could refer to the entire Internet these days). The various implementations differ, but many may struggle after traffic exceeds 50-80Mb/s. You can easily imagine how this could be exceeded at peak by a typical E-commerce configuration with half-a-dozen large servers with multiple 100Mbs NICS running modern three tiered application serviced by a couple of big pipes.

This can be easily rectified with network technology, if you know about it - if. Many operating systems don't even report dropped packets in promiscuous mode (which is why many IDS are implemented on BSD-based operating systems which do) but even if your chosen platform does, some IDS ignore this event. And if the IDS you use doesn't warn you that you are dropping packets, you'll remain blissfully ignorant and not bother to upgrade your infrastructure. It is quite likely that first indication that something is amiss will be when the IDS misses an attack and you get hacked.

Hackers have been reported to have exploited this combination of relatively low traffic capabilities of some NIDS (compared to full-duplex Gigabit switch networking) combined with no through-put alarm - It certainly is possible and there are hacker tools that attempt to flood the network to take advantage of this. However, there are more sure-fire ways that almost guarantee that your attacks go undetected - after all it is pure luck, which packet is dropped and which is processed. If these attacks do work, it's probably because the poor analyst is moribund in log messages and gone home with a headache.

Fragment re-assembly

Oh, no It's basic Network theory - fragmentation occurs because some networks can transmit large packets and some can only transmit very small packets - this maximum size is known as Maximum Transmission Unit (MTU). The Network layer (IP) of the router between these two networks is responsible for taking one large packet and splitting (fragmenting) it up into lots of small bits that will fit down the wire of the tinie-tiny network - this is shown below (figure 1). These fragments will be re-assembled and passed up to the transport layer on the destination host but in-between, the datagrams are fragmented and may even arrive out of sequence.

This can cause some problems for applications that make assertions about the meaning of the data enroute. As one packet may not contain all the relevant data. Good state-full inspection firewalls overcome this by re-joining the original fragments in memory and using this copy of the data to base it decisions on. The process is called virtual packet reassembly.

A good IDS must also use virtual packet reassembly otherwise it could miss important information. Imagine an IDS that worked on the principle of good old Courtney - by reading in a simple packet trace, 1 record at time, looking for indications of hacking. In the un-fragmented attack in the example below, if it searches for the string msadc it will find it with no problems. But in the fragmented example, the string msadc doesn't exist in any single packet so the IDS will miss the attack. Dealing with single fragments will not detect all attacks.

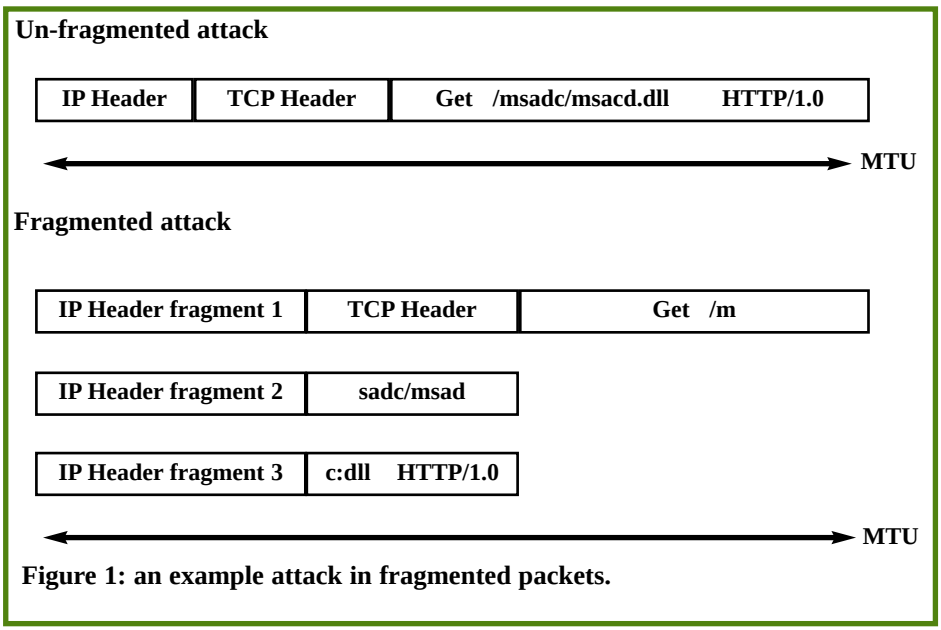


Figure 1: an example attack in fragmented packets.

Enterprising hackers have become aware that some products do not cope with this too well and have created proxies that can take a data streams from TCP or UDP attacks and fragment the packets to avoid detection. The most famous of these is Fragrouter which was effective.

Packet greping, v's Protocol analysis or Just not working right

For a NIDS to work effectively, it has to understand and interpret the data sent in exactly the same way to the destination server and service. This is a "warts and all relationship" that must take into account the reality of how the real servers behave to strange input. If malevolent commands can be sent to servers that will result in an exploit, the IDS must recognise it as an attack even if the data is not constructed to the correct protocol specification or breaks-the-rules - this is not a cricket match, the IDS is there to keep the bad guys out.

In some cases it is as simple as recognising that some servers will treat "get /etc/passwd" equivalent to " GeT /etc/passwd", if the end-point server is smart enough to adjust the case of the command get and remove leading spaces, that's exactly the behaviour the IDS should have when interpreting the attack. Many technical books refer to this as protocol analysis (i.e. interpreting the packet according to the protocol). This is opposed to just searching each packet for a unique attack signature, oblivious to protocol or any other context. This latter technique is known as Packet Greping (Grep being Unix speak for find).

For me, if the IDS doesn't pay appropriate regard to the context of the protocols in transit, it just ain't working right. Here are a number of techniques that highlight the problem.

Hack	Avoidance technique/Description
Port Scanners	Many IDS recognise a port scanner after about 2 or 3 ports within a set period time (a matter of seconds). If you use the IDS avoidance options within a fine tool like MingSweeper, your scans may not register If you really want to defeat most IDS position, spoof your source address and alter it for each port - See side panel
Encoding	For a properly working Web server GET /cgi-bin/ HTTP/1.0 is equivalent to GET /%63%67%69%2d%62%69%6e/ HTTP/1.0A simple text match could miss this.
////////	These exposures are not just restricted to www, ftp servers have peculiarities that may trick the unwary i.e GET /etc/ passwd /tmp/attackinfo is equivalent to GET //////////etc/passwd /tmp/attackinfo
/./../	Everyone knows that ./ means in this directory, so that /./../cgibin/testcgi is equivalent to/cgibin/testcgi Simple but it can fool many an IDS. It is also a nice little resource consumption attack, try it and notice your response times drop.
\cgibin\testcgi	Some web servers don't care what delimiter you use to denote a directory structure. So: \cgibin\testcgi is equivalent to/cgibin/testcgiThis doesn't work on IIS servers but it works on many others.

See sidebar 2 for common avoidance techniques.

Poor Deployment

A poor workman always blames his tools, but even the best chisel will become blunt if you use it as a screwdriver. Likewise even an excellent IDS may not react to significant attacks because of the environment.

Switches

The advantage in using switches is that traffic between any two servers gets a nearly dedicated channel - it doesn't share. This is opposed to a hub where servers share the channel between each connected server. NIDS rely on eavesdropping on traffic passing through a shared segment like a hub. Plug a NIDS into a switch and it will only see broadcast traffic or its own control traffic.

Obviously this is a fundamental problem but fortunately not an insurmountable one. If you need to deploy a NIDS, you have the following choices:

- Use a spanning port - a spanning port is a dedicated port that is linked to one or more normal data ports on the switch. Each time one of these data ports receives a packet; the spanning port receives a copy. This works

perfectly satisfactory on small under-utilised networks with powerful switches. On larger networks, the overhead on the switch might cause problems plus most switches have restrictions on the number of ports which can be bound in this way.

- Tap technology - a Tap is an in-line device that provides a method of directly viewing traffic on a full-duplex or half-duplex 10/100 Ethernet segment. Typically, the Tap is a hardware device that copies the electronic signal - like a "Y" splitter for a TV aerial. It add virtually no delay to the network but can rapidly leave you with a huge tangle of wires.

- Use a NIDS switch card - some switch manufactures also make IDS software. These integrate with the switch by capturing data from the "trunk" or data-bus, which provides minimal performance impact. These are very popular for switched installations but do require some Complex configuration.

SSL

SSL and Encryption has always been one of our best weapons in the security armoury. However, it causes more than a few problems for designers attempted to deploy NIDS. Consider the attacks already described in the section above. Those that involve contacting ports and the services behind them, which are now categorised by those that like to categorise things as context attacks, can be usually identified by the content of the packet header. Firewalls, which are generally far better configured than they were five years ago, block the majority of these. They are also completely unaffected by SSL which only encrypts data payloads not packet headers.

Content attacks, where the attack is contained within the data payload, are another story. My feeling is that these attacks are now the main focus of any intruder - and they are far more deadly. In a normal case (Figure 2), in an HTTP based attack, IDS can detect these.

Unfortunately, as SSL encrypts the data payload of a packet, this blinds the NIDS. Consider all e-commerce and banking apps on the Internet, they are all encrypting because they are most critical but they are just as vulnerable to JILL as any other app. Our NIDS can't tell us when these attacks are being launched because the attack is wrapped in a 128bit encryption envelope. In short most of the attacks launched are being missed because our own security mechanisms. See Figure 3.

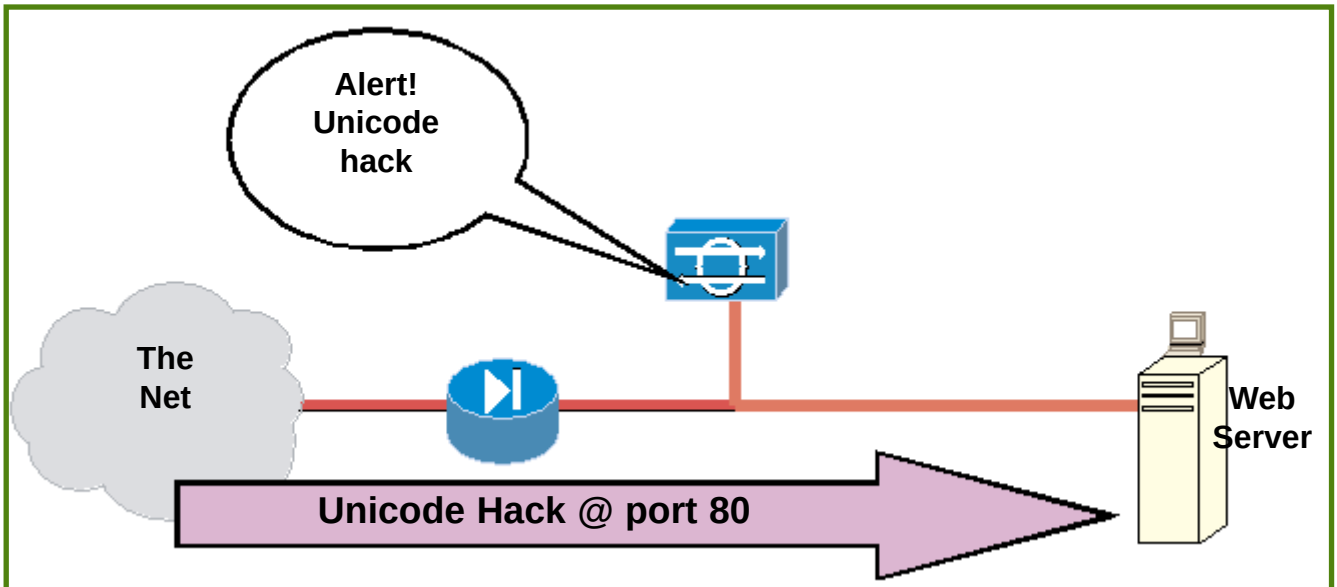


Figure 2: Typical attack with SSL

The only solution I have for this is to use an SSL-Accelerator as the encryption-endpoint as in Figure 4. This does have a few disadvantages but does allow the network for malevolent traffic to be detected. The main disadvantage is that use of client side certificates can become very difficult, since the webserver never receives the details. This is not true when the encryption-endpoint is a reverse proxy but I am becoming a big fan of appliance technology.

Poor Configuration

When I have been called to help out recover hacked systems, the sites always had an IDS installed. So why did the IDS not discover and help the site prevent it. I think there are three main

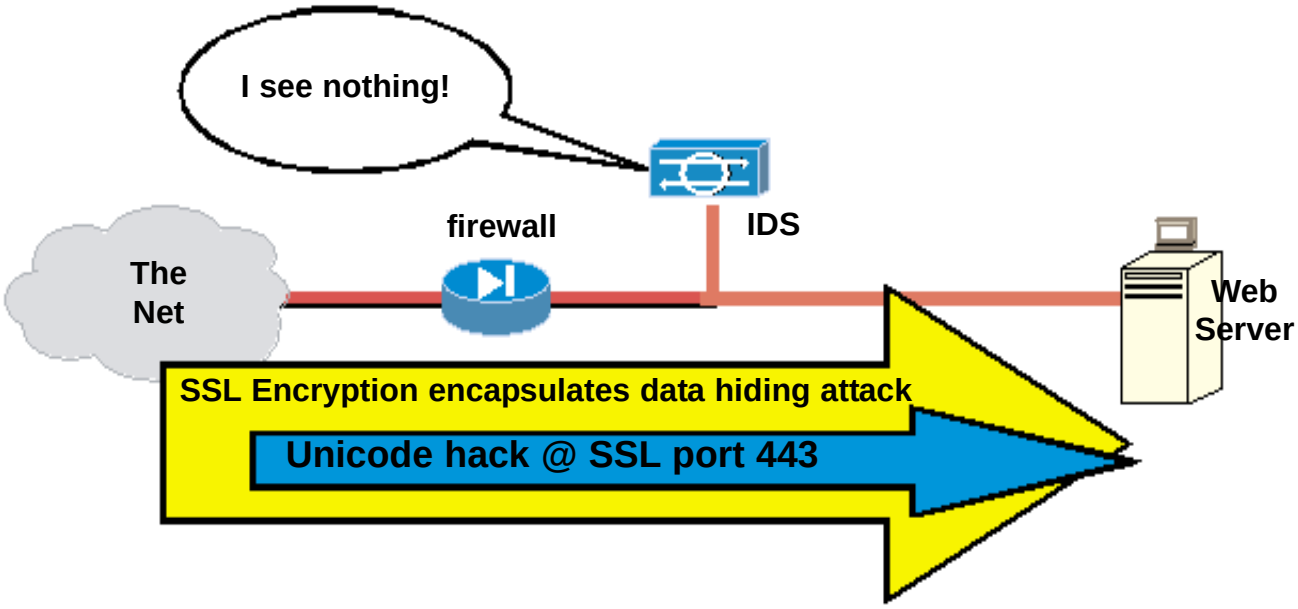


Figure 3: Attack hidden within SSL

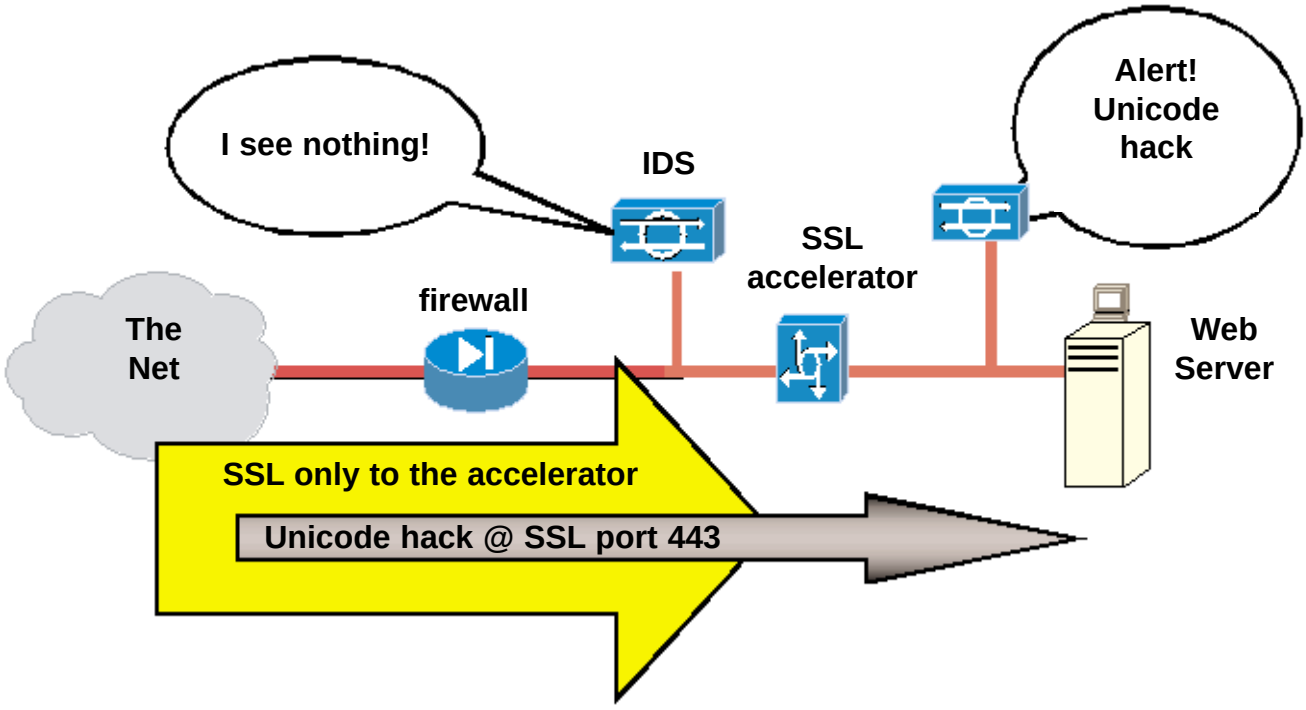


Figure 4: Detecting an attack within SSL

reasons:

- The SSL problem above is very significant;
- The staffs reaction is often ineffective; and lastly
- The IDS detection method is deficient.

There are two main types of detection.

Signature analysis

Most IDS these days use attack signature detection. This is very similar to the approach used by virus scanners. Key patterns are identified in the data and header for a common attack - this might be a particular flag/ID in headers or even a URI string in the data. The IDS sits on a network sniffing packets and reacts when the data matches one of these patterns. Given that the IDS designer is not incompetent, this can be a remarkably effective way of looking for at least the initial overtures of a hacker.

But here's the crunch - Does it detect successful attacks where an intruder invades your network?? **Or does it just report on attacks that should have failed anyway??**

Lets face it, in most cases you will have to configure your NIDS to look, for example, the Unicode hack. So you'll configure your IDS to look for a command like: -

GET /scripts/..%c0%af../winnt/system32/cmd.exe?
/c+dir+c:\inetpub\wwwroot

Which, if successful, will allow you to execute arbitrary commands on an IIS server.

But the key point here is that **you must be aware of this hack to set the IDS looking for it**. For this to happen, in most IDS you'll have to have downloaded a new attack signature and as a security professional you would have read about the subject on the CERT and bugtrack website, right?!

But before you did all this, you would have almost certainly (unless you are mad!) installed the server patch if it were available. You may have even blocked it at the firewall if your implementation has a content or CVP facility. So you are immune to this hack, when the hacker tries it and the IDS goes beep What have you learnt?? Not a lot - "That someone launched an attack that you were immune to."

Not convinced yet? Well think about the first time an attack occurs in the wild, before anyone has designed a signature for it - how does the signature IDS help here. (what would you say to burglar alarm that didn't go-off when first offenders break in). Or what about those vast majority of hacks that does NOT involve a unique "attack" but results from merely poor configuration. You know the ones, telnet open to the perimeter router (with a default password), which in turn can let you telnet to the management server to allow maintenance - we've all seen that sort of thing. None of these events can be uniquely packaged in a neat and tidy signature - but they are examples of Successful attacks in actions that will not be detected by vulnerability signature alone.

Hopefully, I've made the point that signatures alone aren't enough but don't smash up your IDS with a hammer just yet. Experienced practitioners like us know that for large organisations patches can take some while to get deployed - standard builds will have to be amended to avoid regression and there are always those independently maintained servers. And what if the patch doesn't work with all combinations of your software, so you can't patch your servers. NIDS pay you back in this instance by:

- Providing advanced notice that a perpetrator is targeting a particular server with an attack. And these days with 80% of attacks being content attack where the attack is contained within the data payload, rather than context attack, this might not detectable with just firewall logs.
- You also get the opportunity to be proactive in re-action to the attack. If no patch is available, you may choose to reset the connection or shun the source address. This may provide adequate protection, those with NIDS will remember that such techniques really saved their bacon when SYN-flooding was a bright shiny attack.

But however useful this maybe, it is not detecting an unwanted invasion of your network - it is not intrusion detection - it is monitoring your networks for certain attacks. We need something more!

Anomalous traffic detection

This extra sometime is - Anomalous traffic detection and it works by triggering an alert when traffic that should never occur is detected. This may not always be evidence of hacker - it could be a webserver administrator making changes in a non-standard manner, by say not using the staging server. However, it is not understood and much maligned:-

"There are different types of anomalous traffic detection" said the nice young man in a expensive suit from the NIDS manufacturer, " Statistical anomaly and Profile based". He then went onto explain that the first has not been adopted by mainstream manufacturers. He then had a good giggle, pointing at a clipart representation of a firewall (complete with brick-walls topped with dancing flames) with a DMZ and explained to the audience that the second approach was ridiculous - After all, how is any administrator to know what traffic is Atypical or Anomalous. That's why we don't support it.

Unfortunately his product, my favoured commercial NIDS, does support it and had I not been configuring it with a profile of unusual/suspect traffic for many years perhaps I might have been

more convinced too. After all its common sense - for years tools like Portsentry have been reporting on connections that should never have been made. Read a typical description of a hack, when the hacker finds he has the capability to execute commands on your web server he will try to either download his favourite tools often with tftp. If he can't, he will try to gain access to other servers or the firewalls. Surely, failed telnet attempts from your webserver to your firewalls or external tftp traffic are worthy of investigation even if they turn-out to be false alarms.

And as for the NIDS experts remark asserting that firewall administrators and designers can't know want is unusual traffic on a perimeter network segment, Consider the following:

- Typically when designing a DMZ, one or more firewalls are positioned to behave as choke points to restrict network traffic. Also, it is common place to control this by firewall rules, that exactly define what is allowed into/out of the segment - traffic passing through these points that doesn't conform with these rules would certainly be some kind of unusual.
- A good designer would also provide for maintenance access from an administrative LAN or designated management server hopefully via ssh. So maintenance style access like ftp, telnet and Rlogin in between servers or the firewalls would be a good indication that an external party might be attempting to escalate his zone of control.
- Lastly if all else fails, a few UNIX commands like "tcpdump | cut | sort | uniq" slightly enhanced with the correct command line augments (forgive me but I have left them out for the sake of brevity) would provide a nice little summary of what occurs in the DMZ.

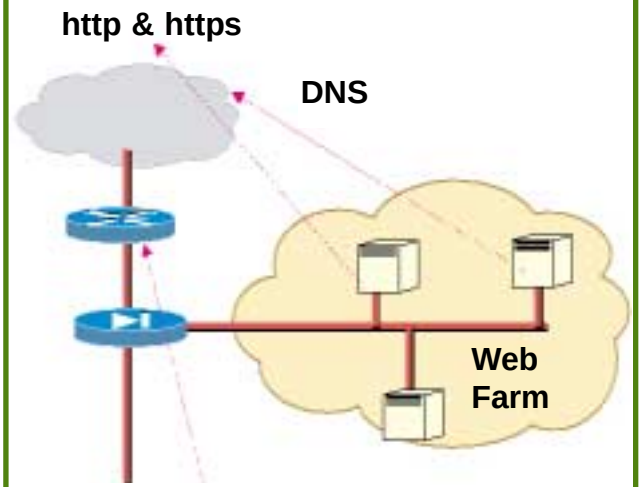


Figure 5: legitimate traffic

So you have your normal traffic profile, you can develop an Anomalous traffic profile. But don't fall into the trap set by the man from the NIDS manufacture, you are not trying to document every unused port that someone may inadvertently contact. Focus on hacker-favoured protocols. In a typical average E-commerce configuration as in figure 6, you could probably assert:

1. TFTP or ftp traffic would not normally be initiated from a webserver to external random addresses;
2. SNMP traffic from application servers to perimeter routers is unusual;
3. Telnet access would not normally be initiated from inside the DMZ particularly not to your firewalls; and
4. site banned protocols like rlogon, NFS and netbeui should not simply appear in your DMZ.

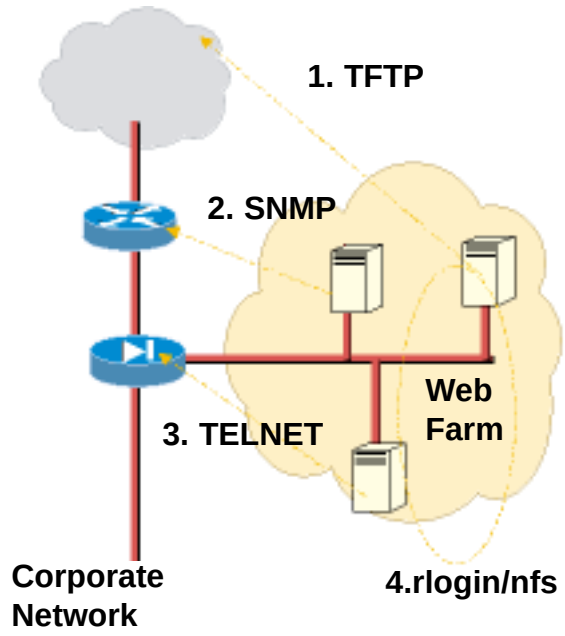


Figure 6: Traffic indicative of unauthorised traffic

Simply code these assertions under into your IDS (by using the Connection tab or by using a combination of connection signatures & filters) and you're be in a position to pick-up all sorts of interesting stuff.

What's the recommendation then?

Profiling takes time to design and even longer to tune - during that time you might be unprotected. Signature analysis tells you about well-known attacks that should have failed because you've patched your servers (not a trivial task, if you run a large organisation). So which is best? Well that is a

Continued on page 16

NETWATCH

ANNABEL LANE takes a peek at the ISACA websites around the world. The Internet Resource List is on page 28

Hello and welcome to another Netwatch. I've recently been looking at the websites belonging to other chapters - first we looked at the parent website in the US in edition 51 and then last edition we looked at the UK chapters' sites. This time I thought we'd go a bit further afield and look at a selection of sites from other chapters around the world to see what resources they have that might be interesting to us.

As you would expect the bulk of the chapter web sites are based in America, so it seemed like a good idea to take a look at a few of those first.

http://www.sfisaca.org - San Franciso Chapter

The San Francisco Chapter's site has an opening picture of the Golden Gate Bridge and when you click to enter it takes you through to the home page proclaiming that this chapter, like our own, is an award winning one. A lot of the emphasis seems to be on careers, which is, after all, an important subject. For example in the resources section there is a section on career guidance which links you through to a choice of several career based sites giving guidance on CVs, information on jobs in the market, etc. There are also in the downloads section presentations available for download from the Chapter events which seem to be all day affairs with a presentation in both the morning and afternoon. There are interesting topics such as TCP/IP control, ORACLE, UNIX, network security, etc. There is also a link to a whole host of other resources, from sites on Disaster Recovery to articles and FAQs on firewalls, for example. If you are looking for something specific, it may be worth trying here.

As you'd expect there is also information on Chapter events and how to sign up for them, the Chapter Directors, CISA, ISACA, etc. All in all a nicely presented site and quite easy to navigate around.

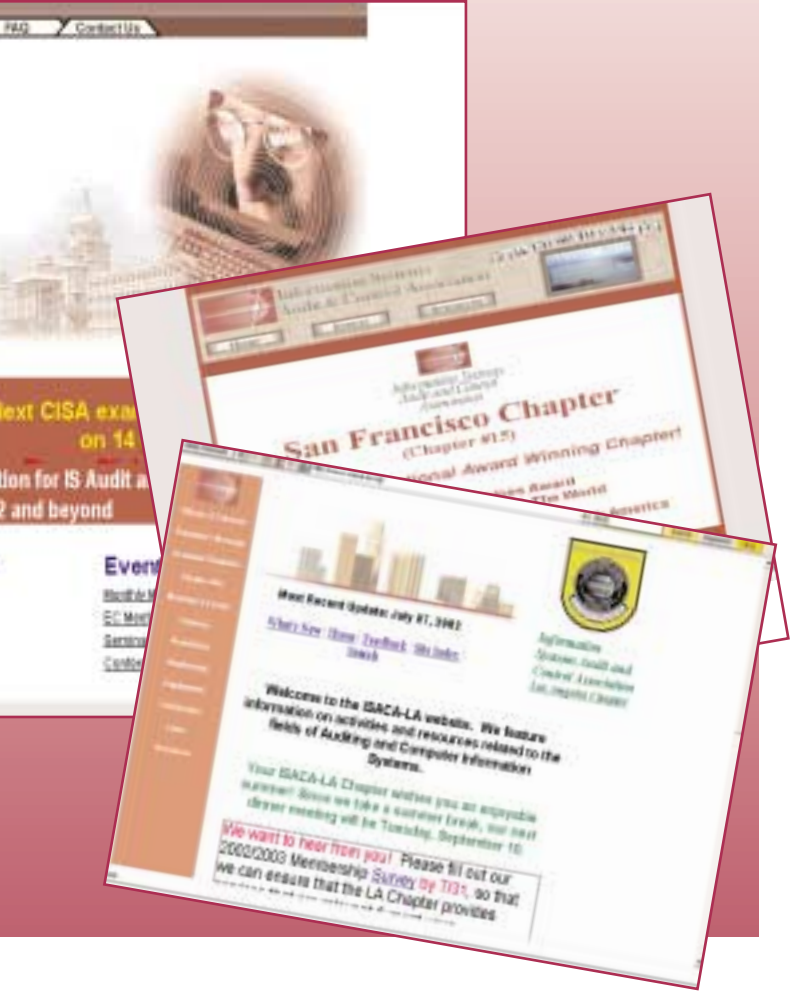
http://www.isaca-la.org - Los Angeles Chapter

As you'd expect there's a lot of activity on this chapter's web site. They have dinner meetings (interesting to see the different kinds of seminars that are out there!) though they have a summer break which was going on when I was on the site for this review. These meetings are discussed in the "What's New" section which gives an overview and you can also download a copy of the presentations given. There's also information on this section on the Spring Conference, a members survey, and they are planning on releasing a directory of all members' details as a members directory.

Of course there's a resource list, which has links to various areas such as the General Audit Office's proclamations, information on continuity planning, etc, but not a large list of links really. There are quite a few more sites in the links page, but again not as many as for some of the other chapters.

http://www.isaca.org.au - Sydney, Chapter, Australia

This nicely laid out front page has a professional look and feel and also acts as a link through to the other Oceania ISACA Chapters, from Perth in Western Australia to Papua New Guinea. News items such as who to contact to register for CISA are on the front page. There are the usual sorts of features such as a listing of the Board members, introduction to ISACA and the benefits of CISA, etc. There are not too many links and a great many of them link you back through to the main ISACA.org website for the other chapter URLs and information on ISACA such as COBIT, although there are also links to the IIA both internationally and in Australia and the Audit Net. The monthly newsletters are supposed to be held on line, but there only appeared to be two there when I visited and the most recent of those was from 2001. I quite liked the Books and Articles page on which members are invited to submit presentation papers on relevant subjects like Application Security, Web security and E Fraud. All of these can be viewed by any visitor to the site with Acrobat and some did look



useful and of interest.

http://www.isacabangalore.org - Bangalore Chapter, India

Time to go a bit further afield I think and India seems quite a long way! When logging onto the site provided by the Bangalore Chapter, the first thing that struck me was its professional lay out with very smart banners and pictures. At the top pf the page is the ISACA mission statement and just below a moving "What's new" banner. This contains scrolling information on job opportunities to exhortations to check the membership list and ensure that your name is on it. There's also a "What's new" button and clicking this takes you through to information on the CISA results, conferences and a newly added links as well as a PKI audit programme available for download.

The front page itself holds a lot of information, on the chapter itself, its history, who the directors are, the number of members, etc to information on the CISA exam which seems to be a common feature of all the chapter web sites. The information on CISA is very comprehensive and also pertinent to the country. Under events there is information on their monthly meetings, conferences and seminars, but the downloads are not here - they fall under the next section - se the next paragraph.

Under the Flash headline you can access their newsletter, which is called "Infocity Auditor", published 6 times a year and is in a mailshot format with an article added to it. When I visited only the February edition was available and this was issue 2.

There is also a link to downloads and there is a lot available here. The first section is downloads from the Bangalore chapter itself from presentations at the Chapter meetings and these cover such topics as risk, CISA success and hacking techniques. The second consists of presentations that they have culled from other chapter web sites and downloads from ISACA itself on auditing standards. All in all this is a well presented web site with plenty of information.

http://www.cadvision.com/isaca - Calgary Chapter, Canada

As you might expect, Canada is also relatively well served with ISACA Chapters with web sites and I trawled a few before settling on reviewing the one from Calgary. It was going to be Montreal which purports to be bilingual, giving the viewer the choice of French or English, but even when you have clicked on English, most of the information still appears in French, so not knowing the level of linguistic skills enjoyed by the readers of this magazine, I decided to play a bit safer and go for one that does at least use English as a communication medium! (By the way there are plenty of chapters out there in other languages ranging from Czech to Thai if you are interested!)

Calgary Chapter's home page has its navigation buttons conveniently placed at the top of the screen. Below are splashes for seminars and conferences which were out of date when I visited, but you can download the presentations which are informative and look as these meetings are held in a lively style! What appears to be the equivalent of our membership meetings are held at lunchtimes - I wonder how that works out as time is clearly quite limited? Under the events button there is further information and members have to pay as well as non members. Again there are presentations to download in some instances. They cover topics such as Business Continuity, the insecurity of Wireless networks, and even such topics as "Take yourself lightly, take your work seriously". Sounds rather deep! This is all held under the "resource" button.

The chapter newsletters are also held on line under their own separate button, accessible form the home page, but when I visited the most up to date was from the end of 2001, which was a bit of shame. It's another award winning newsletter though and runs to several pages, including information about the chapter and a technical article.

In an article of this length, this can only be sample of the chapter web sites that are available. For a full list of all the sites, log onto the ISACA home web site, http://www.isaca.org/ and click on the link to chapters and then to chapter web sites.

Continued from page 13

question you don't have to answer - use both, and get the best of both worlds. The extra effort in deploying will be more than offset by the time wasted by false-positives.

Conclusion

This article sets out some of the common mechanical problems of IDS and their operation. Consideration to problem areas mention will repay you ten-fold. Don't get convinced by the plug'n play or the Zero Cost of ownership myths that are commonplace at the moment.

Please don't get scared off by the problems either - for those connected to the Internet and who have any kind of investment in IT kit or data (that's all of us, isn't it), it is going to become an essential technology. More than anything, it is a fun and fascinating technology which will give you an insight on what is really going on out there - spend a few hours in front of the Event-Console.

Side bar 1: stealth port scanning

Below is a script which will allow stealth port scanning.

```
#!/bin/ksh
#  stealthscan
#
#  example scan with ids avoidance
#  Position yourself on a hub that is on the routable  path to a
#  "C" class network. Between your firewall and  the perimeter
#  router is fine you don't need a real ip  address this script then
#  does an nmap  scan with  spoofed  source address
#
target=10.0.0.1
port=1
saddr=2
# loop thru incrementing $port 1 thru 1024
# also      increment $addr 2 thru 254 and use it to build host
#           portion of "C" class  spoofed network
#
while [ $port -lt 1024 ]
do
#
# Tcp syn scan $target with spoofed address
nmap -sS -S 192.9.200.${saddr}  -P0 -p $port -e eth0 $target >>
tcp.out 2>&1
#
# UPD scan $target with spoofed address
nmap -sU -S 192.9.200.${saddr}  -P0 -p $port -e eth0 $target
>> udp.out 2>&1

sleep 5
#                       increment $port
port=`expr $port + 1`
#                        increment $addr
saddr=`expr $saddr + 1`
#                        reset to 2 after 254
if [ $saddr -gt 254 ]
                        then
                        saddr=2
                        fi
done
cat tco.out udp.out
exit
```

Side bar 2: common ids avoidance techniques as implemented

Below this is the raw output of RFP's whisker utility which show the IDS avoidance available

```
$./whisker.pl -?
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --

-n+ *nmap output (machine format, v2.06+)
-h+ *scan single host (IP or domain)

-I 1 IDS-evasive mode 1 (URL encoding)
-I 2 IDS-evasive mode 2 (/./ directory insertion)
-I 3 IDS-evasive mode 3 (premature URL ending)
            -I 4 IDS-evasive mode 4 (long URL)
-I 5 IDS-evasive mode 5 (fake parameter)
-I 6 IDS-evasive mode 6 (TAB separation) (not NT/IIS)
-I 7 IDS-evasive mode 7 (case sensitivity)
-I 8 IDS-evasive mode 8 (Windows  delimiter)
-I 9 IDS-evasive mode 9 (session splicing) (slow)
-I 0 IDS-evasive mode 0 (NULL method)

            (Note: proxy/bounce support has been removed until
v2.0)
```

Mark Osborne - the Director of Security, KPMG

Mark established KPMG's Technical security function 8 years ago to meet the growing need for practical E-commerce security advice, at a time when you had to invent the security tools used, whether they were used to hack or secure a system. His team, many of whom are well known in their own right, have a long track record of success in delivering security services to most leading UK financial institutions.

He advises many UK institutions on managing their security - he also has substantial technical experience in Internet, E-commerce and M-commerce security, having developed many of the technical security services at KPMG. He has an in-depth knowledge of many commercial firewalls, Intrusion Detection Systems and PKIs.

CISA Training 2003

Information Systems Audit and Control Association

The London Chapter is pleased to announce that in 2003, not only will we offer our well established CISA review weekend workshop, but we will also provide formal training for each of the CISA domains. This additional opportunity to enhance your knowledge in order to help you pass the examination will be provided as 4 one day events. You can either attend all of the days (and receive a 10% discount on the individual day cost), or book individual sessions to suit your particular training needs. All training will include a printed delegate pack and all refreshments.

A maximum of 24 delegates can be accommodated for each training day and the weekend workshop and there is certain to be a huge demand, so book early to guarantee your place.

Venues & Accommodation

Training day sessions will be held in the superb Quorum Training facilities at Tavistock Square, near Euston, in London.

The Residential workshop will be held at KPMG's superb training facilities at Wokefield Park, near Reading.

Email Nancy (nancy@isaca.org.uk) for further details and a registration form

21 January 2003

DOMAINS 1 AND 6

- The IS Audit Process (10%)
- Business Application System Development, Acquisition, Implementation & Maintenance (16%)

25 February 2003

DOMAINS 2 AND 3

- Management, Planning & Organisation of IS (11%)
- Technical Infrastructure & Operational Practice (13%)

31 March 2003

DOMAIN 4

- Protection of Information Assets (25%)

30 April 2003

DOMAINS 5 AND 7

- Disaster Recovery & Business Continuity (10%)
- Business Evaluation & Risk Management (15%)

10 - 11 May 2003

CISA REVIEW WEEKEND

The CISA Review Workshop is a separate chargeable event and its intention is to enable a delegate to identify any particular weaknesses in time to allow remedial action before the CISA examination. The format is primarily a reminder of the core subjects in each domain followed by a mock examination. The actual CISA examination is scheduled for Saturday 14 June, so delegates have a full month to review any weaknesses identifed during the workshop.

The workshop includes Saturday night accommodation and meals.

Different Disclosure Directives Don't Discriminate!

The Data Protection Minefield

Derek Oliver

This is a very difficult subject to discuss, not because of the factual content, which is admittedly both complex and confusing, but because it is almost impossible to write about Acts of Parliament without appearing to make political points. Let me make it clear, right at the start, that ISACA, the London Chapter and Derek Oliver do not have, and do not wish to have any political involvements or bias and anything in this article which may appear critical of Government is purely coincidental and should be read as such. I thank you !

This started out as a review of the recent issues relating to the Regulation of Investigatory Powers Act, RIPA to its friends (Grim Ripa to its enemies), but as the proposed amendments "by statutory instrument" were dropped by the Home Secretary I felt it was less relevant. However, I recently had an enquiry about some possible consulting work in looking at the implications of RIPA in the Data Protection Act (DPA) and that reminded me of some other work I did a while back on the Mental Health Act.

The problem is, where do our organisations stand when the DPA says "thou shalt not disclose" and other legislations says "Thou must disclose". Therein lieth the minefield !

Mental Stimulation

Hospital Trusts and other NHS organisations are obviously good examples of those who hold "personal information" as defined by the DPA. Not only the standard name and address, but some very personal stuff on medical conditions, treatments etc which nobody would like to be publicly available. The confidentiality of patient data is not only, therefore, a requirement of the DPA but is also entwined within the codes of practice of qualified medical and nursing staff and individuals can literally lose their certificates to practice if they are involved in unauthorised disclosure.

Imagine the confusion, therefore, when the Mental Health Act (MHA) comes along and says they must disclose information on an individual's condition as well as demographics to certain people under certain conditions.

Of course, the justification is quite reasonable. Those involved in a person's welfare, be they social services, medical or nursing, ought to be aware if that individual has a medical or mental health condition which may affect not only their treatment but also the way in which they are approached but from the Trust point of view, passing "patient confidential" outside of Trust control, e.g. to the local Council's social services department, is a breach of the DPA although a requirement of the MHA !

Enter the "Sweeney"?

Then, of course, the field gets widened by RIPA. In short, this opens the door for organisations (including telecommunications companies, ISP's etc) holding or processing personal data, i.e. that covered by the DPA, to enable it to be disclosed through monitoring to "certain people under certain conditions", in this case, the forces of law and order - Police, Customs & Excise, Security Services etc - whatever the DPA says about penalties. So, at first view it's damned if you do and damned if you don't; disclosure is in breach of one Act and non-disclosure in breach of another.

Again, a not unreasonable concept for us law abiding individuals: should not the Police etc be given every tool to help them catch criminals ? Note, I am trying hard to avoid any comment on the "rights of the individual" as put forward by various human rights organisations; let's stick to the facts. For a start, there is more legislation to consider.

Let's hear it for Freedom?

RIPA is not alone in requiring disclosure and providing a framework for it: there is also the Freedom of Information Act, 2000 (FIA), which has a code of practice providing "guidance to public authorities as to the practice which it would, in the opinion of the Secretary of State, be desirable for them to follow in connection with the discharge of their functions under Part I (Access to Information held by public authorities) of the Freedom of Information Act".

The FIA recognizes that the disclosure of information following a request may affect the legal rights of a third party such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights. Where the consent of the third party would enable a disclosure to be made an authority should consult that party prior to reaching a decision, unless it is clear to the authority that the consent would not be forthcoming.

But what if it is not forthcoming ? The FIA allows information to be disclosed without consultation if the views of the third party can have no effect on the decision of the authority, for example, where there is other legislation preventing or requiring the disclosure of this information. Legislation such as the MHA or RIPA. Furthermore, a public authority may consider that consultation is not appropriate where the cost of consulting with third parties would be disproportionate !

What's on the horizon?

To be really topical, we now hear that the Government is considering some kind of Identity Card (by whatever name it's called). The possible implications for data sharing resulting from such a card are boundless. Inland Revenue, Customs, Social Services, Department of Employment, Police, MI5/6 and all sorts of Qango's come to mind. A sort of "UK Loyalty Card" perhaps ? Sorry, that's getting to sound "political", but in fact the concept of controlling disclosure of personal data under such circumstances, let alone the technical issues they generate, is quite horrific. Ah well, it all makes work for the auditor to do, as the song goes.

So where's the control?

Let's get one thing straight, the RIPA is intended to be a control rather than an open door. Its opening clauses state "It shall be an offence for a person intentionally and without lawful authority" to intercept anything either in the post or on any public telecommunications system (Section 1.1). Then 1.2 goes on to include private systems.

What it does is provide criteria, notably in Section 6, by which a warrant can be granted for such interception, specifying the individuals who are empowered to apply for such permission. These include:

- The Director-General of the Security Service
- The Director of GCHQ
- Chief Constables and Commissioners of Police

Continued on page 26

Having left wireless networking alone for one issue, well, almost, I am compelled to return to write about this wonderful technology again. Last month I had my car stolen from our drive. The overstretched police didn't seem particularly concerned and as it wasn't the first time unwanted guests had decided that my possessions should be theirs I've recently been studying surveillance systems.

I thought that if I could at least record the next intruder, I could send the video off to Crimewatch and get the culprit. One nice bit of kit that took my fancy was an Axis 2120 network camera. This has motion detection and delivers video directly over a network. It's a sort of webcam with its own internal webserver - just plug in a network cable and you're away.

The trouble is its difficult to get new wires across the car parking area and so I had to look for a wireless solution. That's when the D-Link Wireless Network (802.11b) Video Camera took my eye. Again, it has a built-in web server and although you can configure it to take automatic snapshots at regularly intervals, you can get add-on motion, magnetic, or infrared sensors which enables the camera to take snapshots of triggered events. Incredibly. it also includes e-mail notification to inform you the instant a picture is taken. I know that similar devices are often used in offices for surveillance. Its expensive, but so much easier to install than fixed wired cameras, because you don't have to touch the building infrastructure - just plug it into a power socket. Then I became aware of the on-line forums which exchanged information on where such cameras had been set up in a totally unsecured way. This allows anyone to pick up the radio signal. It seems that some people are then relaying these onto the open web. So much for firewalls. Apparently there are lots of such camera signals that you can watch over the internet with the organisations blissfully unaware that their personal lives are being broadcast live. I don't think that the people who do this can be called 'intruders' as they are simply watching the signals that others are sending to them. Cameras are only one of the new uses found for wireless networking. I read recently how doctors at St Thomas's Hospital have fitted twenty patients with wireless networked pacemakers. These pacemakers send a text message if a patient develops a problem. This seems to me just the start of what is going to be available on the airwaves.

Talking about intruders, I was reading that more than 26,000 computer intrusion incidents were reported to CERT than in the first three months of this year, surpassing the total for all of 2000. Despite government bodies and businesses putting in stronger security in order to protect mission-critical operations and even with legislation being introduced calling for more severe penalties for those who break into computer systems, there are still many high-profile teen hacker cases being reported.

It seems that the widespread availability of easy-to-use scripting toolkits, technical information readily available on the net and lots of spare time to learn new skills tempt teenagers to give cybercrime a go.

" Mafiaboy" used such scripts to bring down targeted sites, and analysts believe hackers created the Anna Kournikova virus with a scripting toolkit.

With more than 30,000 security-oriented Web sites exist, from underground forums to security reporting centres, there is little limit to what can be found out on system vulnerabilities. Most kids wouldn't throw a brick through a shop window, but the teen hackers don't equate defacing a website with smashing a shop window. Personally, as a father of four teenagers (past and present), and as someone who remembers being a teenager, I can't see legislation being the key to stopping teenagers doing what they shouldn't. Sorry guys, you're going to have to secure your networks.

The Career Column

Adrian Simpson

We are now well into 2002 and it is perhaps a not inappropriate time to provide an update on market conditions for computer audit and security professionals.

The last year, out of the fifteen that I have been doing this job, has perhaps been the most economically uncertain that I have known. In past years there has been little doubt that either the economy was growing or was in recession. All one can say at present is that there might have been a recession in the major industrialised economies and in spite of a number of significant economic imbalances, the indicators in the UK and more particularly internationally have become more positive.

Whatever may have happened to economic growth in the UK, and the employment numbers have remained at historically robust levels, many people reading this column seeking work will have felt that the economy was in recession. There is no doubt that 'their' part of the economy has been, and most likely remains, in recession.

If it was not obvious, it certainly is now, that employment in computer audit and security is more dependent on IT spending than on the overall health of the economy. During the early 1990's, during the last real recession, neither computer audit and security employment or spending on IT critical systems was significantly affected. In the run up to Y2K and immediately after, when the implementation of new systems was widely suspended, in spite of robust economic growth, the demand for computer audit staff fell away. It recovered only to fall back again during the latter half of last year when IT spending fell.

The reasons for the correlation between employment opportunities and IT spending are three fold.

First, increases in IT spending translate into new systems developments, an area where most computer audit departments concentrate a significant part of their efforts. Major new systems developments often result in additional demand for permanent or contract resources.

Second, computer auditors are often seconded or permanently transferred into positions in IT that are created as a result of new IT spending. This results in replacements being sought and translates into vacancies.

Third, the demand for external consultancy services increase with spending on IT and consultancies are now major employers of computer audit and security specialists.

Whilst I would not ignore what was happening in the wider economy, IT spending is related to corporate profitability. If I was looking for a talisman for improvements in the recruitment market, I would probably look at the share prices of companies such as Microsoft, Sun and Oracle. When they report increased revenues, improvement in the computer audit market will not be far behind.

The story at the moment therefore remains a lack of demand rather than, with the exception of Andersen, people being forced into the recruitment market. This has been exacerbated by two major sectors, the London banking market and the big 5, or perhaps now big 4 consultancies restricting their recruitment to a minimum. The lack of demand, allowing for a steady supply of people who naturally flow into the market, has resulted in the balance in the recruitment market favouring those who are recruiting. Whilst this has not significantly impacted salaries in the permanent market, other than taking the steam out of the somewhat more ambitious demands, it has certainly hit the rates available to contractors over the course of the last year. Rates available to the large number of security specialists are down by 40% and perhaps 20% for the smaller, less liquid, computer audit contract recruitment market.

It is important to remember that markets are dynamic. There may have been a time when working in computer audit was considered a one way bet and that the demand for your services would always be robust. The last two years have been a bruising experience for a number of people working in computer audit and security. In what has become a more competitive recruitment market it is important to be able to compete effectively for the available positions. For example, you should ensure that you have completed a relevant professional qualification such as CISA and are as far as possible technically up to date.

There is every reason to believe that within the next twelve months IT spending will begin to rise. The dynamics that have resulted in chronic shortages of computer auditors will be reasserted and computer audit will return to the one way bet it has always appeared to be.

Both Internal and External auditors regularly make recommendations concerning computer audit logs. These recommendations are often based around enabling logging on specific systems and ensuring that logs are reviewed on a regular basis. Enabling excessive logging often leads to an information overload and result in the data not being examined properly, if at all.

Systems and Logs

Within the typical corporate environment, the systems that generate interesting logs can principally be divided into two categories: viz., Internal and External.

Internal systems are those which support the day-to-day operations of internal functions and are only normally directly accessible by internal staff or business partners. Internal systems also include those that provide outbound access to the Internet and other external networks. These logs include Windows Authentication, DHCP (Dynamic Host Control Protocol) Address Assignment, Firewalls, Proxy Servers, Business Applications, Databases, Intranet Servers, NetWare Logins, UNIX System logins and Business Partner Systems.

External systems are those that support access by individuals outside the organisation, either as members of the general public or partner organisations. These systems may also support outbound access to the Internet or other networks, which for the sake of simplicity we will consider as separate entities. Logs generated by the externally facing systems include Routers, Firewalls, IDS (Intrusion Detection Systems), Web Servers, Load Balancers, and Application Servers.

Log Volumes

However, it is worth noting that indiscriminately enabling computer audit logs could impact on the performance of the system and, in some cases where disk space is exhausted, may cause the system to fail. Logs from Web Servers, Firewalls and IDS systems can easily amount to more than 100MB per day. Where multiple systems are deployed this can easily amount to more then 1GB of data each day.

Log Consolidation

Analysing in excess of 1GB of logs per day is beyond the scope of most organisations. Assuming that it takes 2 seconds to review each log entry, 1 GB of logs would take in excess of 194 days to review. In addition, analysing each set of logs separately does not allow the most effective use of the available information. By consolidating logs based on a common reference point and analysing the records as transactions pass through the system the most effective use of the information can be made.

For the purposes of data consolidation, date/time is the only common reference point that systems can utilise. To effectively consolidate the variety of logs that each of the systems is generating, the systems must rely on an internal clock that is accurately synchronised against the other systems. To achieve this an external and accurate time source is required; GPS, Radio and Atomic clocks are all available which support the Network Time Protocol (NTP). Version 3 of NTP also provides integrity through the use of the Data Encryption Standard (DES) and RSA Message Digest (MD5), to reduce the risk of an attacker. Version 4 of NTP further enhances this using Autokey public key cryptography.

Log Analysis

With a common reference point between the systems generating the logs it becomes possible to bring all the data together into a single database. Once the logs have been brought together some automated analysis can be performed to identify patterns which may be evident within the consolidated logs. Given sufficient storage space it may be possible to identify patterns extending over significant time periods. This may allow attack reconnaissance to be detected or identify the precursor to a major virus attack.

Conclusions

Therefore, in implementing smart logging controls and processes for system access and transactions against emerging good practice, organisations can reduce the risks associated with performance degradation and non-availability of key systems. In addition, detailed analysis of the consolidated log information can provide an effective tool for detecting unauthorised access, system abuse and normal system/application errors.

Smart Logging

Neil Jarvis
Deloitte & Touche

For further information please contact:

Yag Kanani - Deloitte & Touche
Partner, Information Security Services
+44 207 303 8124.

Question:

How much security is necessary for home PC with access to the net?
http://www.itsecurity.com/asktecs/jul1802.htm

Response from Keith Osborne, ICL

There is no single answer to this, because only you can decide how much security is necessary. You do this by firstly considering what it is that you want to protect - and this may well include your data, your software and, ultimately, your hardware. You then need to identify the threats and vulnerabilities present. Then you need to work out what the risks are, and how you are going to deal with those risks - for example, ignore them, because they are small, or proactively do something about then. From this, assuming that you will be managing at least some of the risk, you will be able to formulate how you will manage the risks - for example, installation of encryption if other people will be using your PC and the data is very sensitive, installation of anti-virus/content filtering software, in case you download a virus from the Net.

That should give you some idea as to how you go about getting an appropriate level of security for your own particular circumstances, but ultimately the amount of security necessary can only be decided by you.

Response from Kevin Townsend, ITsecurity.com

The traditional answer for home computing is that you need at least anti-virus and a personal firewall. There are some, however, who say that this isn't enough. Anti-virus can't detect new viruses, while there are always routes through a firewall (there have to be, otherwise you wouldn't be able to access the Internet nor send or receive e-mail). Such people say you also need some form of intrusion detection to look for anomalous behaviour inside of the firewall. One product that provides both firewall and IDS for the home computer is BlackICE from ISS.

However, you should also include some form of access control to prevent unauthorized people using the computer (friends, neighbours, and even relatives checking to see who you've named in your Will). There are some sophisticated products on the market - or you could limit it to a BIOS password (see elsewhere in the Clinic).

If cost is an issue, you can always periodically scan your PC for viruses with ITsecurity.com's free online virus scanning service (see the Virus Information Center on the home page).

Response from Roberto C. Arbeláez, an IT Security Consultant

I've compiled a small list of online vulnerability scanning web sites.

In any of those pages, you can check out your machine's security in real time, as well as if there are Trojan horses installed, and some other interesting stuff.

I find them very valuable PC vulnerability assessment tools, with the advantage that you don't have to install any vulnerability scanners or any software at all... and they scan both windows and UNIX/Linux machines with excellent results.

Some of them work with NMAP, others with ICMP, some perform stealth port scans...
Here it is:

http://www.sygate.com/scan/scan_req.htm
http://www.linux-sec.net/Audit/nmap.test.gwif.html
http://www.blackcode.com/scan/
http://www.dslreports.com/scan
https://grc.com *(inside the ShieldsUP! Section)*
http://www.csnc.ch/onlinetests/index_e.html
http://www.auditmypc.com/freescan/prescan.asp
http://crypto.yashy.com/nmap.php

Response from Dave Shore, Dave Shore Consulting

All depends on how much you value your PC and its contents along with how much time you intend the PC to be connected. It can also depend on whether anyone else in the house is likely to use the PC and what you want them to be able to access (i.e. children). There are many products around ranging from ZoneAlarm (free last time I looked) to McAfee VirusScan Online and Norton AntiVirus. The latter 2 also provide good personal Internet firewall protection products as well. Many factors have to be considered, but the baseline is protect yourself as best as you can afford if you want trouble free (from viruses and attacks that is) surfing.

Question:

What kind of security risk are home users exposed to when connected to Internet? What are the possible forms of defence against such risk/s and how the defensive measure addresses the risk/s?
http://www.itsecurity.com/asktecs/jul2602.htm

Response from Simon Jenner, Trinity Security Services

Home users are at significant threat from Internet attacks and present an easy target for attackers. A lot of corporate employees are issued with laptops and use them from home to connect to the Internet, this puts corporate security at a huge risk. These laptops often have a very low level of security and can act as a backdoor into a corporate network. Home users are subject to viruses, Denial of Service attacks, data theft and full compromise.

The best way to mitigate the risk is to install personal firewalls on all home and remote user machines. BlackICE from ISS is a good product for this.

Response from Alfred Lau, Computer Advisors

Whenever your computer is directly connected to the Internet, you are putting your computer at risk. Since joining a vast wide area network (the Internet) your computer can expose many vulnerabilities such as viruses, worms, port scanning, net sweeping and many others nasty things. First, a good countermeasure would be to have a anti-virus such as Norton AV or McAfee. Next, to close the "open-doors" of your computer you need to install some sort of firewall. There are free ones like, ZoneAlarm, but if you want more flexibility then you need to purchase ones like the ZoneAlarm upgrade or BlackICE, Checkpoint SOHO version.

Response from Chris Cook, Security Awareness, Inc.

Home computers are often at more risk when connected to the Internet than company-based computers. Many companies are now starting to implement security policies for users performing their work from home. When company information is on these home machines, or even company-owned laptops used at home, there is a factor of risk involved. In the office, we are protected by firewalls, proxy servers, centrally controlled and updated virus software, URL or content filtering, etc. At home, the end user is responsible for all of these safeguards.

Before connecting to the Internet, make sure that your anti-virus software is properly installed, running correctly, and up-to-date. Install a personal firewall such as ZoneAlarm or BlackICE. If you are on a constant connections such as DSL or cable modem, consider an additional layer of a router. Most of these also have their own "firewall" software built-in. When browsing the Web, stick to sites that are well-known and reputable. If you browse adult, gambling or other sites, you are leaving yourself open to malicious or spy code being potentially installed on your machine. Make sure your browser is set to a fairly high level of security.

These days, e-mail can pose an even greater risk. Most viruses are now e-mail based. They are spread as seemingly harmless attachments and infect the machine when the user opens or executes the attached file. Some even execute themselves when the e-mail message is simply opened. Do not use the message preview panel if your e-mail program offers one. Do not open messages from unknown users, especially if there is an attachment. If you get an attachment from a known sender, scan it for viruses before attempting to open or execute it.

Hopefully these guidelines will help to keep you and your information safe.

Response from Robert Schifreen, Information Security Training Ltd

How long do we get to answer this question? Are we allowed to write on both sides of the paper?

The risks are that, when you're connected to the Internet, anyone in the world can connect to your PC. Depending on what programs you're running, and which security patches you're *not* running, the hackers can do all sorts of stuff. The only sensible defence is a firewall, and software ones like ZoneAlarm are pretty good. Read the information on www.zonelabs.com for more.

Response from Keith Osborne, ICL

Very similar risks that office users are exposed to - being connected to untrusted third parties - i.e. potentially anyone on the Net - the Net does not distinguish between geographical or physical locations. These risks are, in summary:

- Corruption or destruction of data
- Loss of integrity of software
- Fraud
- Breach of applicable legislation, for example DPA 1998
- Denial of service

continued from page 19

- Commissioners of Customs & Excise
- "A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom"

Whilst the last may appear to be somewhat subjective, the point of section 6 is made and, effectively, restricts and controls who can even ask for access to interception. The recent issues discussed to death, and subsequently dropped like the proverbial hot cakes by the Government, were based on plans to increase this list to include various bodies which would appear to have more limited responsibility for law and order.

You'll probably remember that this list included local authorities, Inland Revenue and all sorts of organizations down to and including the Milk Marketing Board (let's get the swine who don't drink their daily pinta !).

So, at the moment, RIPA is not necessarily our first concern as audit and control professionals.

What can we do?

Well that's the problems, disclose or not disclose depending on which legislation appears appropriate. But what am I suggesting you, dear reader, might do about it ? Simply, be pro-active and do something right now.

I suggest that you look at the personal data you hold in your organizations, perhaps as an add on to an audit of DPA compliance ? What data are you holding and for what purpose, that, after all, is the basis of DPA registration so will be assessed as a part of your audit.

Once you have the data, look at what legislation, MMH, RIPA, FIA, could possibly affect you and how you could address the demands of that legislation. The target is to have a formal protocol, a set of internal criteria by which data can be disclosed. Call it an extension to your Information Security Policy if you like. In brief, it is a template which those responsible for data confidentiality can apply if they are faced with a demand for disclosure which will protect your organization from action for non-compliance with the DPA.

You'll need to incorporate the rules which apply to your data under each of the Acts so that nobody is in any doubt as to what can be disclosed to whom and under what circumstances. The point is to do it now, not wait for the situation to arise because that's how mistakes get made leading to unauthorized disclosure and prosecution with all its attendant publicity etc.

Let's be careful out there !

ISACF Research Activities

The IS Audit and Control Foundation carries out important research on behalf of its members. Research is the lifeblood of an organization like ISACA - it ensures that the Association is at the leading edge and its members are well-equipped to tackle emerging risks. Here is a brief update of the current projects you can look forward to. This is followed by some ways in which you can help out:

1. **Privacy Management Guideline** - The author of this publication is a Research Board member, Robert Parker Partner at Deloitte and Touche, Canada.
2. **E-commerce Security** - The publications nearing completion are Network Perimeter Security for E-commerce and Application and Business Continuity in an E-commerce Environment
3. **Wireless Communication Security and Control** - This covers Security and risk management in wireless communication networks, and the researcher is being done by Wheeler Associates.
4. **Customer Relationship Management (CRM)** - This will covers security, integrity and control in CRM systems and the research is being carried out by PricewaterhouseCoopers, Chicago.
5. **Electronic/Digital Signature Law Survey** - This is a comparison of all pertinent world wide laws covering electronic and digital signature laws. It has been authored by volunteers from the Research Board and will be available on the ISACA website
6. **Net-trading Exchanges** - This is a joint research with the Canadian Institute of Chartered Accountants (CICA) The research will be carried out by Deloitte and Touche, Canada.
7. **Enterprise Resource Packages (ERP) Integrity** - This will cover security, integrity and control for SAP, Peoplesoft and Oracle, and the researchers are Deloitte Australia. At the moment, the SAP publication is at review stage, and Oracle and Peoplesoft will be completed in July 2002.
8. **OS/390 Security-Z/OS** - This is a technical reference guide to information security in an OS/390 environment (major changes from MVS). The researcher is Peter Tingsted in Denmark. The project will be complete at the end of second quarter 2002.
9. **Oracle RDBMS** - This is an update of a 1993 ISACF monograph, and will include the latest Oracle release, and is the is an update that the ISACA bookstore has the most requests for. Research will be performed by PwC, and will include Internet related issues up through version 9i of Oracle.
10. **Enterprise Information Integrity** - This is a quantitative and qualitative research into the risks and techniques for information integrity, along with a framework. Some funding will be provided by Unitech, and the researcher will by carried out at the Centre for IS Assurance at University of Waterloo in Canada.

Potential Future Projects - The ideas of the Chapter members are always welcome, so please submit your ideas to research@isaca.org.

Funding Requirements - In order to continue producing high quality research, the Foundation and Research Board need your financial support. Some others ways in which members can help are:

- Chapter financial support
- Organizations and Individuals willing to provide funding
- Volunteers willing to work on complimentary basis or royalties
- Organizations seeking revenue sharing arrangements
- Organizations seeking direct funding
- ISACF funding

Kamal Khan

K-NET is an Internet-based database of knowledge specifically developed to provide members with direct access to current knowledge references relevant to information systems governance, control, security and assurance.

For K-NET, pertinent knowledge has been sought, identified and peer-reviewed, then organized into logical categories of interest to ISACA members and other constituents. Composed of Internet references to articles, books, education and web sites, K-NET includes:

* Full access for ISACA members
* 12 subject areas
* More than 90 topic areas
* Over 1500 knowledge references
* Weekly updates
* Search engines
* Personalization features

K-NET's personalized service enables members to remain current on the topic areas most important to them. K-NET can automatically e-mail members on a weekly basis about new database references within their specified areas of interest. To activate this personalized service and register to receive updates on your topics of interest simply visit *www.isaca.org/gir/gir_tuf.htm*. We are certain you will find this personalized service of great value.

K-NET℠

A Global Knowledge Network for IT Governance, Control and Assurance

Visit ***www.isaca.org/knet*** to gain more knowledge about the following subjects:

CISA (CERTIFIED INFORMATION SYSTEMS AUDITOR)
Exam Preparation

IS AUDIT, CONTROL & SECURITY – SPECIFIC ENVIRONMENTS
Active X
AS/400
CGI
CICS
DB2
Directory Services
EDI
HP OpenView
Informix
JAVA
Linux
Lotus Notes
MVS
Novell Netware
OMVS
Oracle Database
Oracle Financials
OS/390
PeopleSoft
RACF
SAP R/3
SMF
SQL Servers
Sybase
SYS1.PARMLIB
Tivoli TME10
UNIX
VAX/VMS
Windows NT/2000

IS AUDIT, CONTROL & SECURITY – TOOLS
ACL
CAATs
IDEA
Methodware

IS AUDITING
Access Control
Accounting Information Systems
Audit Committee
Audit Department Procedures Guide
Cont Audit Guidelines
Computer Applications
Data Center
Ethics
Information Integrity
Integrated Auditing
Outsourcing
Risk Assessment
Standards
System Development
Trading Partners
Value Added Auditing

NETCENTRIC (INTERNET, INTRANET, EXTRANET) CONTROL & SECURITY
Browsers/Servers
Certificate Authorities
Cryptography/Encryption
Data Warehouse
Digital Signatures
E-mail
Firewalls
Gap Technology
Internet Attacks
OLTP
TCP/IP Networks
Virus Protection

IS SECURITY
Biometrics
Computer Crime/Forensics
Data Center
Incident Handling
Information Privacy
Information Security Policies
Local Area Network (LAN)
Security Monitoring

IS CONTROL
Access Control
Cont Control Objectives
Control Self-Assessment
Key Performance Indicators (KPI)
Standards

IT GOVERNANCE & BUSINESS MANAGEMENT
Audit Function
Change Management
Cont Framework/Management Guidelines
Computer Crime
Continuity Planning
Data Warehouse
ERP
Ethics
Executive Information Systems (EIS)
Expert Systems
Governance
Healthcare
Information Privacy
ISO 9000
IT Implementation & Management
Knowledge Management
Mergers & Acquisitions
Performance Measurement
Policies and Procedures
Reengineering
Resumption Planning
Risk Assessment
Strategic Planning

eBUSINESS
E-Commerce
EDI
Legal Issues
Security and Control
Strategies

TELECOMMUNICATIONS
Client/Server Security and Control
PBX Systems
Telecommuting
Dial-up Connection Security
Network Risk and Controls

PROJECT MANAGEMENT
Implementation/Monitoring
Team Development

PROFESSIONAL DEVELOPMENT
Career Planning & Development
End-User Computing

K-NET Access:

Access to all K-NET references is open to current members of the Information Systems Audit and Control Association (ISACA). Limited access is available to all others who seek knowledge of IT governance, control and assurance.

Members add value by identifying new, high-quality web-based knowledge for inclusion in K-NET. Member participation in this endeavor is vital to the ultimate success of the K-NET project and the ultimate value realized by ISACA members. Please e-mail your web site suggestions (including the exact URL) to *knet@isaca.org*.

Do you need additional CPE credits to maintain your CISA certification? Did you know you can earn up to 10 CPE credits for volunteering to help assist in the continued development of K-NET? To earn these additional CPE credits all you have to do is volunteer and participate as a reviewer of potential K-NET web site references. This is a great opportunity for you to truly make a contribution to the profession. For more information on becoming a K-NET volunteer, visit *www.isaca.org/knetvol.cfm*.

K-NET is just one more benefit of your ISACA membership. By providing full access to a knowledgebase covering a broad range of professional IS control, security, assurance and IT governance topics, K-NET keeps you current.

INTERNET RESOURCE LIST

AUDIT
http://www.isaca-london.org
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
www.barclaysimpson.com

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
http://web.mit.edu/security/www/gassp1.html
www.eSecurityOnline.com
http://www.pki-page.org/
http://www.microsoft.com/TechNet/win2000/win2ksrv/prodfact/pkiintro.asp
http://www.sans.org/topten.htm
www.securitywatch.com

COMPUTER COMPANIES AND SYSTEMS
www.microsoft.com
www.alw.nih.gov
ntresearch.com/
www.acl.com/audit/audit2.htm
www.caseware-idea.com
http://www.sap.com/mysap/
www.windowsitsecurity.com

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
http://ecommerce.internet.com/
http://www.ecrc.ctc.com/about.htm