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

JOURNAL
volume 16 number 2 summer 2006 ISSN 1741-4229

Programme of Briefings & Meetings 2006

Title	Meeting type	Date
Computer Audit Basics 4: Application Controls	Late afternoon meeting	Tuesday 24 January
Control Aspects of ITIL (Service Delivery) / Cobit	Late afternoon meeting	Tuesday 07 February
Wireless Technology	Late afternoon meeting	Tuesday 07 March
Latest Developments in IT Law	Late afternoon meeting combined with IRMA AGM	Tuesday 02 May
Spreadsheet Risks: Ubiquity, Severity & Legality?	Late Afternoon	Tuesday 12 September
Lifting the lid on Stolen Laptops	Late Afternoon	Tuesday 3 October
Project control: the auditor's role in IS projects and systems development – joint meeting with ICAEW	Full Day	Tuesday 21 November
TBA	Late Afternoon	Tuesday 5 December

Apart from any joint meetings with other organizations all meetings will be held at BCS, 5 Southampton Place, London WC2
This is a draft programme only and is subject to change. For confirmation of dates and further information, watch the **Journal**, email **admin@bcs-irma.org** or visit our website at **www.bcs-irma.org**

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

Email distribution is here . . .

IRMA has moved from paper to electronic distribution of the Journal, so we need your email address! If you have not already supplied it, please can you send your email address to our admin office at admin@bcs-irma.org with your membership renewal or to the chair at brewer.alex@gmail.com (preferably with the subject "IRMA contact details"). Many thanks.

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

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

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

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

Submission Deadlines

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

PLEASE NOTE THE EMAIL ADDRESS FOR

IRMA ADMIN

IS:

admin@bcs-irma.org

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

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

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

Produced by Carliam Artwork, Potters Bar, Herts

Editorial

John Mitchell

My ISP is anxious to attract new subscribers so it presents these potential income streams with great offers. Cash backs, free wireless routers, discounted period, etc. What do us existing and reliable customers get? Nothing. Moving to a new ISP is pretty straight forward these days and like the interest rate tarts in the financial services sector the urge to move is becoming stronger with each offer that my ISP makes to potential customers. Surely they should start thinking about retaining their existing customer base, especially when one ISP has announced apparently totally free broadband? Okay, there are catches with this offer, but the message is clear. The underlying communication method should be "free" with the profits coming from the provision of value added services.

On the subject of service, I found out that I could now make an appointment with my doctor via the internet. So I registered for the service, very quickly received my access credentials and then tried to do the business only to find that the appointment site was down. So I whizzed off an email to the provided contact address only to receive a response that they could not let me know when the service would be available due to "patient confidentiality" and I should contact my surgery for help! So I blew my top and flame mailed them and received a slightly more reasoned reply that they could not deal with patients because there are too many of us. To which I pointed out that if that was the case why did they provide their contact details on the site? No response, but the service came up the next day and I made my appointment, which is a very useful value added service.

Some of you may have heard reports regarding an experiment conducted last Valentine's day in London. The experiment carried out within London's business district revealed that employees in some of the City's best known financial services companies don't care about basic security. CDs were handed out to commuters as they entered the City by employees of an IT skills specialist and recipients were told the disks contained a special Valentine's Day promotion. However, the CDs contained nothing more than code which informed the distributor how many of the recipients had tried to open the CD. Among those who were duped were employees of a major retail bank and two global insurers. The CD packaging even contained a clear warning about installing third-party software and acting in breach of company acceptable-use policies – but that didn't deter many individuals who showed little regard for the security of their PC and their company.

Fortunately these CDs contained nothing harmful. No personal or corporate data was transmitted due to the actions of these individuals but the fact remains that this could have been someone wanting to cause havoc in the City. Effectively the employees, by carrying the CD into the company and putting it into their PC, had by-passed much of their company's security. Employees have to recognize they are the first and easiest route into a company's network and social engineering of this nature requires no technical skill to bypass the company's firewall. Just last year Japanese bank Sumitomo Mitsui in the City allegedly fell victim to a spy ware infection which almost ended with the theft of £220m. That case should have highlighted the threat posed by applications entering the enterprise through unofficial channels and yet it appears few companies have taken note. The key here is 'education'. Regularly keeping all employees abreast of the latest scams is the duty of the company, it's officers and corporate security team.

Which leads me nicely into the phishing problem. I receive so many of these that when I received a message purportedly from the National Lottery I automatically consigned it to the rubbish bin. After all, it was suggesting that I should follow a link and provide my log-on details. So I dumped it, but a week later I realized that I had not received an expected (small) cheque for a recent win and so logged on to find out why. You will have guessed it already. The message from the Lottery people was to inform me that I had won and the reason for not receiving the cheque was that the money had been paid to my bank account! I had forgotten this last part it being so long since I had won anything, but the main point is that here was a legitimate message being rejected by me because I thought it was a phishing spam. A sort of self imposed denial of service being triggered by my own paranoia!

Which brings me neatly to this edition, where you will find a prediction on phishing activity from Vasilis Katos of Portsmouth university, while Bob Ashton, our Oceania correspondent, deals with the problems faced by IT professionals in keeping up-to-date. Mark Smith provides details of some member benefits he has negotiated on your behalf and Alex Brewer, our chairman provides an update on the Group's activities during the previous year. Jean Morgan our Treasurer gives you an insight to our finances, but Colin Thompson who provided the BCS Matters column for so many years has retired and I am in the process of searching out a replacement, so no news this time from our parent body.

Chairman's Corner

Alex Brewer

Chairman's report for 2005/06

IRMA is 40 (or more)

Depending on who you talk to, IRMA was 40 (or perhaps even more) this year. As such the group, previously called 'Auditing By Computer' and the 'Computer Audit Specialist Group', is the oldest Specialist Group in the BCS.

To celebrate we bought a large chocolate cake (Tesco) and our first meeting of the year was free to all.

Thanks to the committee

Before looking at the round up for the year, I would like to give my heartfelt thanks to the committee who have worked hard during the year to keep IRMA's engines running.

Thank you all for your continued support, ideas, and work.

Number and type of members

During our 40th year, the membership has increased to 201 members, an encouraging sight after the decline of recent years. We have several initiatives to keep up the momentum:

Student membership can be sustained for minimal cost, so in the current year we shall contact universities running courses in IT security and governance related matters to see if students are interested in signing up and attending.

We shall be continuing the 'Computer Audit Basics' meetings to provide material that may be of interest.

Moving away from corporate membership. This is partially to bring the membership system in line with what the BCS can support on their membership system. In the medium term we hope to transfer our records to the BCS.

The use of BCS HQ has also helped the membership feel settled: – these wonderful premises are now known to our members, who are comfortable attending, and the food is good too!

If you hadn't realised, we have now moved all meetings (except for the joint one) on to the first Tuesday of about every other month, except where someone has got in first (as in September). We hope to avoid this in the future.

Programme for the year

- During the year we have run a varied programme
- IS governance
- Mobile computing (with ICAEW)
- Application controls
- The Governance and Control of IT Services using COBIT and ITIL
- Wireless technology update
- IT Law (today)

The meetings I have attended have been well received, even the Mobile Computing one that I was project managing. Despite the loss of a speaker (which I covered for) the event went ahead with good feedback.

Future programme

One more for 05/06 –

Project Control – The Auditor's Role in IS Projects / Systems Development

Projects consume major amounts of organisations' time and money: if we 'follow the money' this mandates us looking at projects. This event will be on the 6th June.

06/07

Spreadsheet risk (September 12th) – this key area is one that will not ever go away.

It is also very likely that the following will take place:

- Joint event with ISACA and ICAEW (subject to be agreed – in November)
- Probable evening on 'SAP for beginners' (Date TBA)

Email distribution

During the year we have also persuaded all of our members into providing up to date email addresses to enable three important processes:

Contacting our members about BCS ventures - involvement of the members in BCS based projects (the most notable being ID cards and related matters during the last year) is something where both members and the BCS can benefit. Ad hoc requests for informed opinion come from BCS from time to time, however the forwarding of these to the members is something we've not been able to do before.

Distribution of the journal - this is now available as a PDF download from the website. This even allows us to have the journal in colour!

Messages of interest to members - occasionally reduced fee or even free training courses come our way, and sometimes it is frustrating not to make these more widely known. This is now possible.

Reminders for subscriptions – instead of a giant snail mail shot, members can be reminded in a timely and relatively painless (for IRMA) manner to pay their subscriptions.

IRMA's continuing relevance:

I believe IRMA has continuing relevance - here are two topical examples where IRMA can supply the links between the technology and the risks:

the problems besetting the previous Home Secretary (he was still there when the AGM was held) is data quality. The data concerning prisoner location is estimated as 45% accurate.

RFIDs have just been installed in passports. I should know. My eldest daughter's passport arrived two weeks ago without one, and my middle daughter's passport arrived with a RFID tag fitted. So it's brand new. But does the tag work? What data is loaded in it? Who can sweep for and identify the RFID and at what range?

With that, we look forward to an exciting and stimulating programme for 2006/07 – I hope to see you all there.

IRMA MEMBERS' BENEFITS DISCOUNTS

Mark Smith

We have negotiated a range of discount for IRMA members, see below:

Software

Product	Discount Negotiated	Supplier
Caseware Examiner for IDEA (mines security log files for Windows 2000, NT, XP)	15%	Auditware Systems (www.auditware.co.uk)
IDEA (Interactive Data Extraction and Analysis)	15%	Auditware Systems (www.auditware.co.uk)
Wizrule (data auditing and cleansing application)	20%	Wizsoft (www.wizsoft.com)
Wizwhy (data mining tool)	20%	Wizsoft (www.wizsoft.com)

Events

Event	Discount Negotiated	Contact
E-Tec courses (www.e-tecsecurity.com)	10%	Margaret Mason (info@e-tecsecurity.com)
IACON 2006 (www.iir-iacon.com)	20%	Jonathan Harvey (jharvey@iirltd.co.uk)
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine (julie@unicom.co.uk)
Websec 2006 (www.mistieurope.com)	15%	Lisa Davies (LDavies@mistiemea.com)

We are constantly looking to extend this range of discounts to include additional events, training courses, computer software or other products that our members may find beneficial. If you have any suggestions for products we could add to the list, please contact Mark Smith (mark.smith@smhp.nhs.uk), our Members' Benefits Officer, and he will be happy to approach suppliers.

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

Resources

All IS auditors and security practitioners will be familiar with the problem of keeping abreast of fast moving developments in technology.

Unless auditors and security practitioners make serious efforts to keep their knowledge current, it will quickly become irrelevant and may provide a false sense of comfort to clients if auditors are unaware of critical security issues in emerging technologies. A good example is the risks presented by wireless local area networks (WLANs). Auditors with inadequate and out-of-date knowledge and skills may concentrate on the controls within a financial application, while ignoring the fact that passwords providing access to that application are being broadcast far and wide by an insufficiently secured WLAN.

Management also expects those responsible for technical controls, and auditors who review them, to have knowledge that is both current and comprehensive in today's environment. This has led many clients to pressure audit firms to require IS auditors to obtain the Certified Information Systems Security Professional (CISSP) accreditation in addition to the Certified Information Systems Auditor (CISA) designation, as a deeper level of technical knowledge is required to obtain CISSP.

The aim of information security has always been to protect the confidentiality, integrity and availability of information using the processes of prevention, detection and recovery. IS auditors have always laboured under the disadvantage that they are expected to provide opinions on systems which reside on a multitude of platforms, whose attributes are changing constantly. New technologies and software appear, and security features evolve and change with every release. In order to begin to address to aims stated above IS auditors need to develop current knowledge in the following areas:

Background information on technologies under consideration.

Information on security aspects of the technologies under consideration.

Information on certifications in the technologies under consideration, and if necessary obtain those certifications in order to demonstrate their competence.

Resources

Technical bookshops are full of IS manuals similar in size to telephone directories. These sources of information have the disadvantages that they become obsolete with every software release, and the greater part of their contents are not relevant to those needing to focus on security issues.

The following 2 on-line resources, the former being financed by advertising and the latter by sponsorship, avoid these disadvantages and are freely available to everyone:

CramSession Study Guides

These are designed to assist people who are studying to take IT industry certifications. The study guides consist of downloadable pdf files, and are organized as a series of self contained lessons and are available free of charge. More than 270 study guides are available for preparation for the certifications provided by the following vendors and certifying authorities:

- Check Point
- Cisco
- Citrix
- CIW
- CompTIA
- CWNP
- EC-Council
- ISC2
- LPI
- Microsoft
- Network Associates
- Novell
- Oracle
- Red Hat
- Sun
- Symantec
- TIA
- TruSecure

In addition, valuable career advice is provided for anyone considering such certifications. The site also includes "The List", which is a compilation of all the technical qualifications they know about, including links to those certification sites.

Auditors are able to use this resource to focus on the security or other aspects of technologies with which they may be unfamiliar.

Realtime Publications

To quote Realtime:

"Realtimepublishers.com is the worldwide leader in corporate-sponsored e-publishing. We publish high-quality publications, which are free to readers, on the web sites of industry-leading companies around the world. Our publications are published on a chapter-by-chapter basis, as they are written. This unique concept of publishing in "real time" provides readers with the information they need on today's critical IT topics, and our sponsors with valuable content for their web site visitors."

Books are available as downloadable pdfs, either from Realtime's website, or individual sponsors' sites. The books that I have obtained have been well written and of quality content. Many titles are available. The following relate to IS security, and will be very relevant to IS auditors and security specialists.

The Administrator Shortcut Guide to Email Protection

The Administrator Shortcut Guide to User Management and Provisioning

The Definitive Guide to Information Theft Prevention
The Definitive Guide to Controlling Malware, Spyware, Phishing, and Spam
The Definitive Guide to Securing Windows in the Enterprise
The Definitive Guide to Security Inside the Perimeter
The Definitive Guide to Exchange Disaster Recovery and Availability
The Definitive Guide to Active Directory Troubleshooting and Auditing
The Definitive Guide to Email Management and Security
The Definitive Guide to Identity Management
The Definitive Guide to Security Management
The Definitive Guide to Service-Oriented Systems Management
The Definitive Guide to Windows 2000 Security

The ExamPrep Guide to Security Certifications

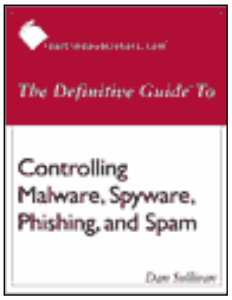
The Practical Guide to Compliance and Security Risks

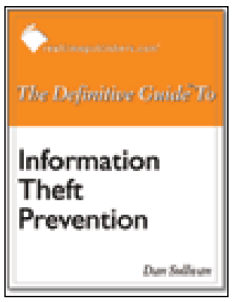
The Shortcut Guide to Automating Network Management and Compliance
The Shortcut Guide to Managing Certificate Lifecycles
The Shortcut Guide to Network Compliance and Security

The Video Guide to Protecting Internet Access and Communications

The Tips and Tricks Guide to Software Security Assurance
The Tips and Tricks Guide to Secure Content Appliances
The Tips and Tricks Guide to Secure Messaging
The Tips and Tricks Guide to Securing Windows Server 2003

For further information:
www.cransession.com
www.realtimepublishers.com





Forecasting Volatility of Active Phishing Sites

Vasilios Katos

Abstract

Although it is suggested that the phishing threat is increasing rather rapidly for financial institutions and consumers, this analysis performed on data from the Anti-Phishing Working Group (APWG) shows that the problem of phishing has started showing signs of slowing down. As phishing remains a profitable avenue for attackers, this saturation could indicate that a new wave of phishing attacks, possibly stealthier ones, is about to be unleashed.

Introduction

Phishing, the attack related to "identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" [1] is a fruitful avenue for criminals committing financial related fraud.

Phishing trends are steadily rising [1] and the corresponding financial losses are considerable. It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totalling an approximate $929 million. U.S. business lose an estimated $2 billion USD a year as their clients become victims [2]. The United Kingdom also suffers from the immense increase in phishing. In March 2005, the amount of money lost in the UK was approximately £504 million GBP [3] whereas the total business loss was in the area of £1.3bn [4].

Considering that the damage made by the growing phishing activity is steadily increasing, the purpose of this analysis is to explore the volatility of the number of unique phishing sites detected. A phishing web site is counted unique, when email campaigns sent to multiple users direct them to this specific web site. We argue that once a phishing site has been identified and exposed, the losses attributed to this site are expected to decrease; this is due to the fact that the consumer's position on the learning curve and awareness is high. Therefore the exercise here is to forecast the appearance of new phishing sites.

The analysis is performed on data from the Anti-Phishing Working Group (APWG) and employs the GARCH estimation method used typically to forecast the volatility (i.e. risk) of stocks in a stock market, which makes it an ideal tool for predicting phishing trends.

The data

The data used in the analysis is weekly, cover the period from first week of July 2004 to last week of April 2005, and are taken from the Anti-Phishing Working Group (APWG) [1]. The identification of the variables used is the following:

p_t = number of unique phishing sites detected, shown in Figure 1.

$r_t = ¢\ \ln(p_t)$ = growth rate of p_t, shown in Figure 2.

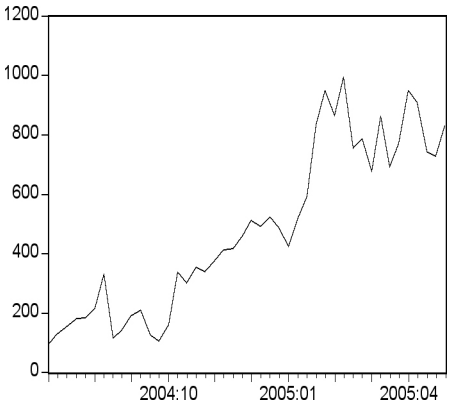


Figure 1 Number of unique phishing sites (r_t)

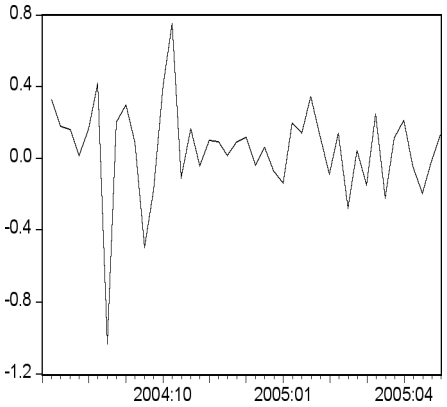


Figure 2 Growth rate of unique phishing sites (p_t)

For variables p_t and r_t to be used in estimation they must be stationary, i.e., the joint distribution of each variable must be unchanged if displaced in time. Appendix A indicates the methodology followed for testing the stationarity of these two variables. It is found that both $\ln(p_t)$ and r_t are stationary. Generally, from the actual data in Figure 1 it can be seen that the number of unique phishing sites detected, p_t or $\ln(p_t)$, is growing, and from Figure 2 it can be seen that the growth rate of the number of unique phishing sites detected, r_t, has certain periods that have higher volatility.

The results

Appendix B shows the detailed generalized autoregressive conditional heteroskedasticity in mean model [11], or GARCH-M, used for modelling variables $\ln(p_t)$ and r_t. As a result of this modelling, the dynamic forecast of $\ln(p_t)$ and its corresponding variance are shown to Figures 3 and 4 respectively. The accompanying indexes that indicate the quality of the forecasts, i.e. the Theil inequality coefficient = 0.0183, Bias proportion = 0.0002, Variance proportion = 0.0513, Covariance proportion = 0.9485, verify that these forecasts are very good.

Similarly, the dynamic forecast of r_t and its corresponding variance are shown to Figures 5 and 6 respectively. The accompanying indexes that indicate the quality of the forecasts, i.e. the Theil inequality coefficient = 0.7252, Bias proportion = 0.0013, Variance proportion = 0.4541, Covariance proportion = 0.5246, also verify that these forecast are rather good.

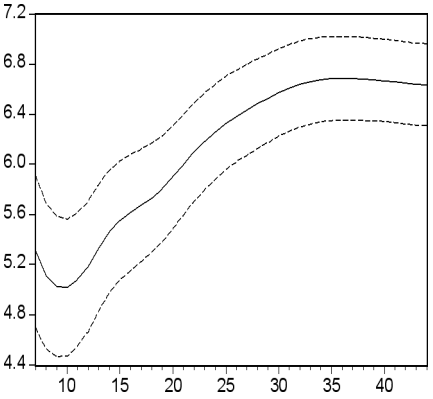


Figure 3 Dynamic forecast of ln(p_t) and its standard errors

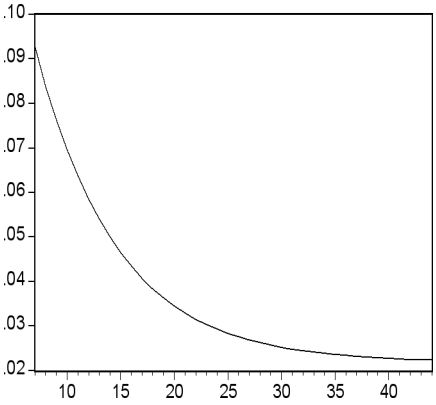


Figure 4 Dynamic forecast of variance of ln(p_t)

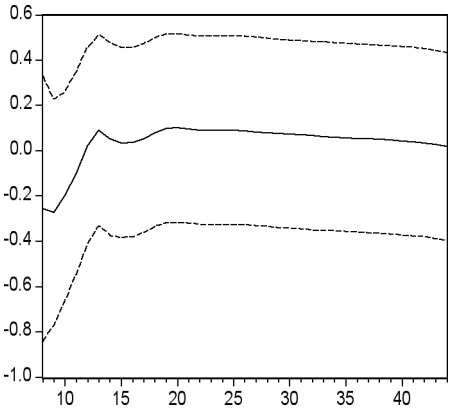


Figure 5 Dynamic forecast of r_t and its standard errors

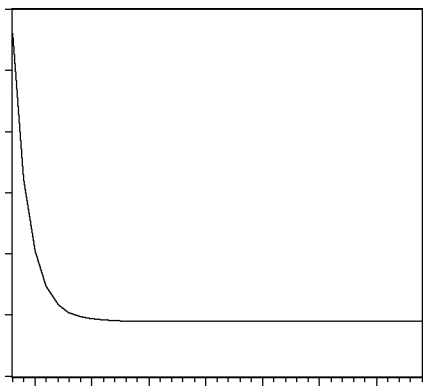


Figure 6 Dynamic forecast of variance of r_t

Discussion and concluding remarks

Although it is suggested that the phishing threat is increasing rather rapidly for financial institutions and consumers and thus conducting financial transactions online may place consumers at more risk, we advocate that the problem of phishing has started showing signs of slowing down. This is because from the estimates in the previous section it is forecasted that the number of the unique phishing sites detected is increasing at a decreasing rate and the volatility (variance) of this number is steadily decreasing, reaching its equilibrium at very low level. This could be attributed to the raised awareness - or alternatively the suspiciousness - of the consumers, combined with the actions of the financial institutions to revisit their authentication approaches. For instance, the use of one's personal data such as date of birth and mother's maiden name for authentication purposes had serious flaws, as such information was not intended to be used to prove one's identity over the phone or the Web. Furthermore, the depreciation of personal data in terms of security is high; the privacy of non-volatile information such as a date of birth for instance, will depreciate with time and its privacy state cannot be reverted. However, financial institutions are adopting authentication approaches in requiring "a memorable date" and "a memorable name" instead of the more personal and non-volatile data. This gives the opportunity for the authentication information to be constantly "fresh" – a concept originating form the discipline of cryptography.

However, this does not mean that additional methods of protection, including new legislation, user training, and technical measures, should be relaxed, but on the contrary this saturation is an indication of a new family of threats and attacks that are likely to manifest.

References

[1] http://www.antiphising.org

[2] P.Kerstein, "How Can We Stop Phishing and Pharming Scams?" CSO, July 19, 2005; http://www.csoonline.com/talkback/071905.html.

[3] T. Richardson, "Brits fall prey to phishing" The Register, 3 May 2005; http://www.theregister.co.uk/2005/05/04/aol_phishing/.

[4] "Stealing the limelight", The Guardian, 17 March, 2005; http://technology.guardian.co.uk/online/story/0,3605,1438851,00.html.

[5] D. Dickey, and W. Fuller, "Distributions of estimators for autoregressive time series with unit root". Journal of American Statistical Association. 74. 1979pp. 427-431.

[6] H. Akaike, "Information theory and an extension of the maximum likelihood principle." In: Petrov, B. and Csake, F (eds.) 2nd International Symposium on Information Theory. Budapest: Akademiai Kiado, 1973.

[7] R. Schwarz, "Estimating the dimension of a model." Annuals of Statistics. 6., 1978. p. 461-464.

[8] T. Breusch, "Testing for autocorrelation in dynamic linear models." Australian Economic Paper. 17 . 1978. pp. 334-355.

[9] L. Godfrey, L. "Testing against general autoregressive and moving average error models when the regressors include lagged dependent variables." Econometrica. 46. 1978.

pp. 1293-1302.

[10] Eviews 4.0. www.eviews.com

[11] R. Engle, D. Lilien and R. Robins, R.P. "Estimating time varying risk premia in the term structure: The ARCH-M model." Econometrica. 55. 1987. pp. 391-407.

APPENDIX A

In examining the stationarity of variables p_t and r_t we used the Augmented Dickey-Fuller (ADF) tests [5]. In order to find the proper structure of the ADF equations, in terms of the inclusion of an intercept (c) and a trend (t), and in terms of how many extra augmented lagged terms to include in the ADF equations, for eliminating possible autocorrelation in the disturbances, the usual Akaikes's [6] information criterion (AIC) and Schwartz's [7] criterion (SC) were employed. The minimum values of AIC and SC indicated the 'best' structure of the ADF equations. With respect to testing for autocorrelated disturbances, the usual Breusch [8] and Godfrey [9], or Lagrange multiplier LM test, was used. Following this methodology, the ADF statistics were found to be as follows:

- For variable p_t: ADF = -3.1744 (significance = 0.1031), intercept c and trend t were used. This means that p_t is not stationary.
- For first difference of p_t variable ($\_p_t$): ADF = -7.9131 (significance = 0.0000), intercept was used. This means that $\_p_t$ is stationary, or variable p_t is integrated of order one, i.e. I(1).
- For variable $\ln(p_t)$: ADF = -3.3468 (significance = 0.0724), intercept c and trend t were used. This means that $\ln(p_t)$ is rather stationary, or variable $\ln(p_t)$ is integrated of order zero, i.e. I(0).
- For variable r_t: ADF = -5.5295 (significance = 0.0000), intercept c was used. This means that r_t is stationary, or variable r_t is integrated of order zero, i.e. I(0).

The analysis above indicated that variables $\ln(p_t)$ and r_t, i.e. variables I(0), should be used in estimation.

APPENDIX B

For modelling variables $\ln(p_t)$ and r_t we started by using the simple form

$$Y_t = \alpha + \hat{\mathbf{a}}'\mathbf{X}_t + \varepsilon_t$$
$$\varepsilon_t \sim N(0, \sigma^2) \qquad (1)$$

where Y_t is the dependent variable, X_t is an n_k vector of explanatory variables, _ is a k_1 vector of coefficients, _ is a constant and $\__t$ is the error term, which is assumed to be independently and normally distributed with a zero mean and a constant variance $\_^2$. However, having only variables $\ln(p_t)$ and r_t we used as explanatory variables in X_t the lagged dependent variables $\ln(p_{t-j})$ and r_{t-i}, and a polynomial of the time trend variable t, in order to capture the effects of possible missing explanatory variables on the dependent variable such as legislation, user training for detecting phishing, technical measures, etc.

The estimation results for $\ln(p_t)$, applying the ordinary least squares (OLS) estimation method, using Eviews 4.0 [10], are shown bellow:

$$\ln p_t = 3.02953 + 0.00297t^2 - 0.00004t^3 + 0.39899\ln p_{t-1} + e_t \qquad (2)$$
$$[4.341]\ [3.423]\ [-3.085]\ [2.822]$$

$R^2 = 0.8928$ $\bar{R}^2 = 0.8846$ DW = 1.8202 AIC = 0.0109 SC = 0.174

LM(1) = 1.4745 White = 9.9906 JB = 12.9459 ARCH = 5.238
{0.2246} {0.1250} {0.0015} {0.0221}

where:

R^2 = determination coefficient

$\bar{R}^2$ = adjusted for degrees of freedom determination coefficient

DW = Durbin – Watson statistic for autocorrelation

AIC = Akaike information criterion

SC = Schwartz criterion

LM(1) = Lagrange multiplier statistic of order one for autocorrelation

White = White heteroskedasticity statistic

JB = Jarque – Bera statistic for normality

ARCH = Autoregressive conditional heteroskedasticity statistic

e_t = residuals

[ ] = t-ratios in brackets

{ } = specific significances in parentheses

Although the results in equation (2) may look acceptable, in fact the JB test suggests that the normality assumption is violated and the ARCH test suggests that the hypothesis of homoskedasticity is also violated. This means that equation (1) is not adequate for modelling $\ln(p_t)$ and other patterns should be used.

Similarly, the estimation results for r_t, applying a moving average MA(1) procedure for the error term, are shown bellow:

$$r_t = -0.03412 + 0.00780 - 0.00019t^2 + 0.37031r_{t-1} + e_t - 0.96888e_{t-1} \qquad (3)$$
$$[-0.890]\ [1.888]\ [-2.053]\ [2.441]\ [-32.489]$$

$R^2 = 0.2944$ $\bar{R}^2 = 0.2182$ DW = 1.8031 AIC = 0.1032 SC = 0.310

LM(1) = 1.7567 White = 5.8702 JB = 10.0338 ARCH = 3.142
{0.1850} {0.3191} {0.0066} {0.0763}

Although the results in equation (3) may look also acceptable, in fact the JB test suggests that the normality assumption is violated and the ARCH test suggests that the hypothesis of homoskedasticity is rather violated. This means that equation (1) is not adequate for modelling r_t too and other patterns should be used.

In cases where the ARCH statistic is significant, indicating thus that there are certain periods that have higher volatility, the most appropriate model to be used instead of model (1) is the generalized autoregressive conditional heteroskedasticity in mean model [11], or GARCH-M(p,q), which is written as follows:

$$Y_t = \alpha + \hat{\mathbf{a}}'\mathbf{X}_t + \theta\sigma_t^2 + \varepsilon_t$$
$$\varepsilon_t \sim N(0, \sigma_t^2) \qquad (4)$$

$$\sigma_t^2 = \alpha_0 + \sum_{i=1}^{p} \gamma_i \varepsilon_{t-j}^2 + \sum_{j=1}^{q} \delta_j \sigma_{t-i}^2 \qquad (5)$$

where _, _o, _i and _j are parameters to be estimated. Equation (4) is usually called the mean equation and (5) is called the conditional variance equation.

The estimation results for $\ln(p_t)$, applying the maximum likelihood (ML) estimation method and a moving average MA(1) procedure for the error term, using Eviews 4.0 [10], are shown bellow:

$$\begin{aligned} \ln p_t &= 11.52201 + 0.445889\,\ln p_{t-1} + 0.037210\,\ln p_{t-2} - 0.000914\,\ln p_{t-3} + 7.72E-06\,\ln p_{t-4} \\ &\quad [23.598]\,[-30.546]\,[49.892]\,[-9.01E+12]\,[68.074] \\ &\quad -0.073695\,PDL01_t + 0.007019\,PDL02_t \\ &\quad [-3.559] \qquad [1.389] \\ &\quad -2.084959\,\varepsilon_t + e_t + 0.193341\,e_{t-1} \\ &\quad [-0.556] \qquad [0.783] \end{aligned} \qquad (6)$$

$$\begin{aligned} \sigma_t^2 &= 0.002270 + 0.398663\,\varepsilon_{t-1}^2 + 0.477598\,\sigma_{t-1}^2 \\ &\quad [0.896] \quad [1.288] \quad [1.717] \end{aligned} \qquad (7)$$

$R^2 = 0.9130$ $\bar{R}^2 = 0.8761$ DW = 1.7154 AIC = -0.1635 SC = 0.353

Q – stat(2) = 0.5949 Q-stat(16) = 9.2035 JB = 1.7217 ARCH = 1.763
{0.441} {0.867} {0.4228} {0.1842}

where:
PDL01 and PDL02 = variables constructed by applying the polynomial distributed lag to $\ln(p_t)$ of lag five and order three, starting at $\ln(p_{t-1})$, i.e. PDL($\ln(p_{t-1})$, 5, 3). Analytically, the corresponding estimated expression it is given by

$$\begin{aligned} &-0.067\,\ln p_{t-1} - 0.119\,\ln p_{t-2} - 0.157\,\ln p_{t-3} - 0.181\,\ln p_{t-4} - 0.191\,\ln p_{t-5} - 0.188\,\ln p_{t-6} \\ &[-4.32] \quad [-5.48] \quad [-8.20] \quad [-11.46] \quad [-5.87] \quad [-2.83] \end{aligned}$$

Q-stat(2) and Q-stat(16) = Q statistics for autocorrelation from 2 to 16.

All the diagnostic tests accompanying estimation of equations (6) and (7) are acceptable, although some coefficients in these two equations are not significant. Therefore, equation (6) can be used for the dynamic forecasting of $\ln(p_t)$ and equation (7) can be used for the dynamic forecasting of the variance of $\ln(p_t)$.

Similarly, the estimation results for r_t, applying the maximum likelihood (ML) estimation method and a moving average MA(1) procedure for the error term, are shown bellow:

$$\begin{aligned} r_t &= -2.313522 + 0.245955\,r_{t-1} - 0.011916\,r_{t-2} + 0.000218\,r_{t-3} - 1.95E-06\,r_{t-4} \\ &\quad [-2.837]\,[9.885]\,[-14.400]\,[126.107]\,[-6.314] \\ &\quad -0.134059\,PDL01_t + 0.023339\,PDL02_t \\ &\quad [-1.228] \qquad [1.333] \\ &\quad +3.225889\,\varepsilon_t + e_t + 0.187441\,e_{t-1} \\ &\quad [0.838] \qquad [0.950] \end{aligned} \qquad (8)$$

$$\begin{aligned} \sigma_t^2 &= 0.019799 + 0.181026\,\varepsilon_{t-1}^2 + 0.312211\,\sigma_{t-1}^2 \\ &\quad [1.031] \quad [0.700] \quad [0.543] \end{aligned} \qquad (9)$$

$R^2 = 0.3186$ $\bar{R}^2 = 0.0188$ DW = 2.1766 AIC = 0.4366 SC = 0.959

Q – stat(2) = 1.0234 Q-stat(16) = 11.555 JB = 0.5309 ARCH = 0.109
{0.312} {0.712} {0.7669} {0.7412}

Similarly, the corresponding estimated expression for the polynomial distributed lag PDL(r_{t-1}, 5, 3) is given by

$$\begin{aligned} &-0.111\,r_{t-1} - 0.175\,r_{t-2} - 0.192\,r_{t-3} - 0.162\,r_{t-4} - 0.086\,r_{t-5} + 0.038\,r_{t-6} \\ &[-1.25] \quad [-1.28] \quad [-1.33] \quad [-1.41] \quad [-1.27] \quad [0.32] \end{aligned}$$

All the diagnostic tests accompanying estimation of equations (8) and (9) are acceptable, although some coefficients in these two equations are not significant. Therefore, equation (8) can be used for the dynamic forecasting of r_t and equation (9) can be used for the dynamic forecasting of the variance of r_t.

Vasilios Katos is a Senior Lecturer and Course Leader for the MSc in Forensic IT at the University of Portsmouth, UK. He received a PhD in Computer Security from the University of Aston in the UK, an MBA from the University of Keele in the UK and an MEng in Electrical and Electronic Engineering from Democritus University of Thrace in Greece. He has also worked for a period of two years for Cambridge Technology Partners (Novell Inc.) in The Netherlands as a security analyst. His research interests are in Information security and cryptography.

email: vasilios.katos@port.ac.uk

School of Computing, University of Portsmouth, Buckingham Building, Lion Terrace, Portsmouth PO1 3HE, UK

BCS IRMA FINANCES SUMMARY 2005/2006

Expenditure (£)			Income (£)		
Membership Admin		-906.35	Membership	3,847.00	
Journal (Summer 05)	-1,668.14		BCS Interest	1,377.25	
Journal (Autumn 05)	-1,244.20				
Journal (Winter 05)	-1,398.25	-4,310.59			
E-Journal (Spring 06)		-611.00			
Admin		-181.23			
Catering (AGM 05)		-146.07	ICAEW (prev yr)	699.45	
			ICAEW (mobile)	174.15	
Admin (18/10 mtg IT Govce)	-685.25				
Catering 18/10	-297.50	-982.75			
Admin (24/1 mtg Audit)	-90.00				
Admin (7/2 mtg COBIT)	-90.00				
Catering 24/1, 7/2	-294.43	-474.43			
Admin (Wireless meeting)		-70.00	Misc meetings income	326.03	
Catering		-76.67			
Speaker expenses		-48.50			
40th Anniversary Committee meal		-365.70			
Web hosting		-74.00			
Total Expenditure to 26/4/2006		-8,247.29	Total Income to 26/4/2006	6,423.88	
Opening Balance 1/5/2005		**£ 25,588.69**	**Closing Balance 1/5/2006**		**£ 23,765.28**

Notes:

1. BCS year ends 30/4. This summary post-dates IRMA AGM and includes all transactions.
2. Membership Admin includes transition costs for emailing journals.

HUMOUR PAGES

Project Management Proverbs

1. It takes one woman nine months to have a baby. It cannot be done in one month by impregnating nine women.

2. Nothing is impossible for the person who doesn't have to do it.

3. You can con a sucker into committing to an impossible deadline, but you cannot con him into meeting it.

4. At the heart of every large project is a small project trying to get out.

5. The more desperate the situation the more optimistic the situatee.

6. A problem shared is a buck passed.

7. A change freeze is like the abominable snowman: it is a myth and would anyway melt when heat is applied.

8. A user will tell you anything you ask, but nothing more.

9. Of several possible interpretations of a communication, the least convenient is the correct one.

10. What you don't know hurts you

11. There's never enough time to do it right first time, but there's always enough time to go back and do it again.

12. The bitterness of poor quality lasts long after the sweetness of making a date is forgotten.

13. I know that you believe that you understand what you think I said, but I am not sure you realise that what you heard is not what I meant.

14. What is not on paper has not been said.

15. A little risk management saves a lot of fan cleaning.

16. If you can keep your head while all about you are losing theirs, you haven't understood the plan.

17. If at first you don't succeed, remove all evidence you ever tried.

18. Feather and down are padding, changes and contingencies will be real events.

19. There are no good project managers – only lucky ones.

20. The more you plan the luckier you get.

21. A project is one small step for the project sponsor, one giant leap for the project manager.

22. Good project management is not so much knowing what to do and when, as knowing what excuses to give and when.

23. If everything is going exactly to plan, something somewhere is going massively wrong.

24. Everyone asks for a strong project manger - when they get them they don't want them.

25. Overtime is a figment of the naïve project manager's imagination.

26. Quantitative project management is for predicting cost and schedule overruns well in advance.

27. The sooner you begin coding the later you finish.

28. Metrics are learned men's excuses.

29. For a project manager overruns are as certain as death and taxes.

30. Some project finish on time in spite of project management best practices.

31. Fast – cheap – good – you can have any two.

32. There is such a thing as an unrealistic timescale.

33. The project would not have been started if the truth had been told about the cost and timescale.

34. A two-year project will take three years, a three year project will never finish.

35. When the weight of the project paperwork equals the weight of the project itself, the project can be considered complete.

36. A badly planned project will take three times longer than expected – a well planned project only twice as long as expected.

37. Warning: dates in a calendar are closer than they appear to be.

38. Anything that can be changed will be changed until there is no time left to change anything.

39. There is no such thing as scope creep, only scope gallop.

40. A project gets a year late one day at a time.

41. If you're 6 months late on a milestone due next week, but really believe you can make it, you're a project manager.

42. No project has ever finished on time, within budget, to requirement.

43. Yours won't be the first to.

44. Activity is not achievement.

45. Managing IT people is like herding cats.

46. If you don't know how to do a task, start it, then ten people who know less than you will tell you how to do it.

47. If you don't plan, it doesn't work. If you do plan, it doesn't work either. Why plan!

48. The person who says it will take the longest and cost the most is the only one with a clue how to do the job.

49. The sooner you get behind schedule, the more time you have to make it up.

50. The nice thing about not planning is that failure comes as a complete surprise rather than being preceded by a period of worry and depression.

51. Good control reveals problems early, which only means you'll have longer to worry about them.

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

BCS
THE BRITISH COMPUTER SOCIETY

Membership Application

(Membership runs from July to the following June)

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

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)*	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: _____	£15
STUDENT MEMBERSHIP – Full-time only and must be supported by a letter from the educational establishment. *(An annual quota is in operation, so IRMA retains the right to close this level of membership at any time).* Educational Establishment: _____	£FREE

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

All communications from the Group are likely to be electronic.

Please tick this box to indicate you agree to be contacted this way. ❑

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

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

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

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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	Alex Brewer	brewera@ebrd.com
SECRETARY	Siobhan Tracey	siobhantracey@aol.com
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Ross Palmer	ross.palmer@hrplc.co.uk
JOURNAL EDITOR	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON – IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON – ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wal Robertson	williamr@bdq.com
ACADEMIC RELATIONS	Vacant	

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	admin@bcs-irma.org

OR VISIT OUR WEBSITE AT	**www.bcs-irma.org**	Members' area Userid = irmalondon Password = 4members06

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of Information Risk Management and Audit by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Direct e-mailing

We can undertake direct e-mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members of £350.

Contact

Administration

Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: admin@bcs-irma.org
Website : www.bcs-irma.org

Meeting Venue unless otherwise stated

BCS, The Davidson Building,
5 Southampton Street,
London WC2 7HA