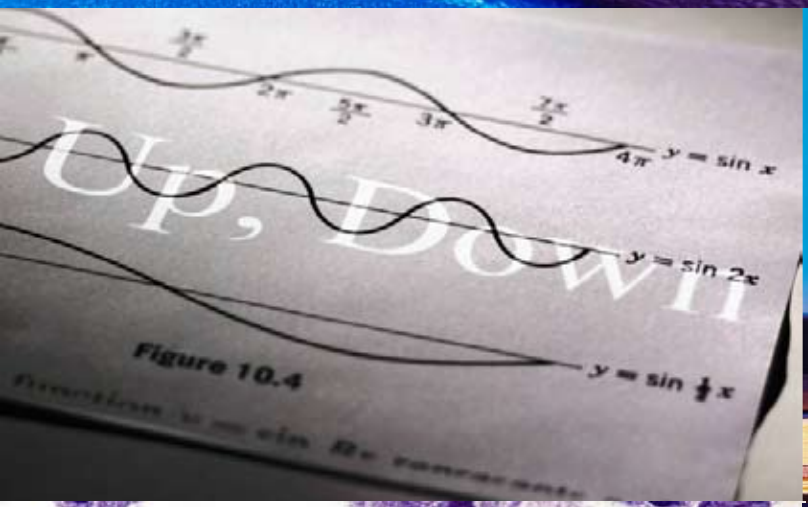
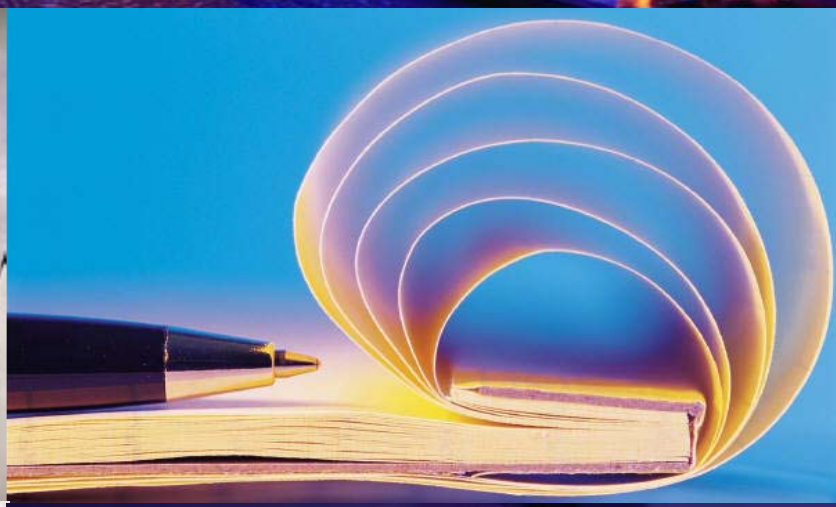
CIAO Newsletter

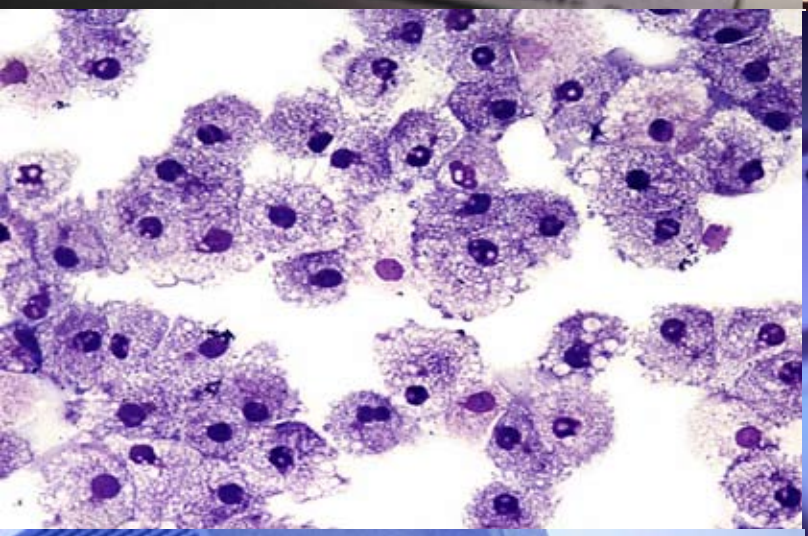
Centre for Informatics & Applied Optimization

Graduate School of Information Technology & Mathematical Sciences, University of Ballarat

University of Ballarat
Learn to succeed







Edition #29 - Spring 2010

Cybercrime Workshop at UB

CIAO's Internet Commerce Security Laboratory (ICSL) recently hosted the **Second Cybercrime and Trustworthy Computer Workshop 2010** in Ballarat.

Cybercrime continues to be an **international growth industry**, assisted by a combination of technical factors such as **insecure hardware and software platforms**, and human psychological factors including **user error and naivety**.

The objective of this two-day workshop was to bring together **two distinct groups** to encourage further collaboration:

1. People **researching cybercrime activity** such as phishing and malware.

2. People working on **technical countermeasures.**

Key participants included:

> ICSL's founding industry partners: Mr Cameron Woolfe (IBM) and Mr Simon Brown (Westpac Banking Corporation).

> ICSL's new industry partner: Assistant Commissioner Neil Gaughan, Australian Federal Police.

> Professor Lynn Batten, Deakin University Chair in Mathematics.

> Mr Stephen McCombie, Centre for Policing, Intelligence & Counter Terrorism, Macquarie University.

Research paper presentations on cybercrime included:

> Professor Lynn Batten, Deakin University: "Classification of Malware Based on String and Function Feature Selection".

> Mr Stephen McCombie, Macquarie University: "Winning the Phishing War: A Strategy for Australia".

Research paper presentations on cybercrime by ICSL PhD students included:

> Ms Amber Stabek: "The Seven Scam Types: Mapping the Terrain of Cybercrime", awarded **Best Paper.**

> Mr Desmond Lobo: "Windows Rootkits: Attacks and Countermeasures".

> Mr Mamoun Alazab: "Towards Understanding Malware Behaviour by the Extraction of API Calls".

> Mr Robert Layton: "Authorship attribution for Twitter in 140 characters or less".

> Ms Kylie Turville: "Understanding Victims of Identity Theft: Preliminary Insights".

Technical Demonstrations included:

> "Rootkit analysis" - Mr Desmond Lobo.

> "Torrent monitoring system" - Mr Robert Layton.

> "Forensic processes used by IBM" - Mr Cameron Woolfe, IBM.

> "Forensic image processing using Matlab" - UB's Mr Mofakharul Islam.

> "Malware analysis" - Dr Lei Pan, Deakin University.

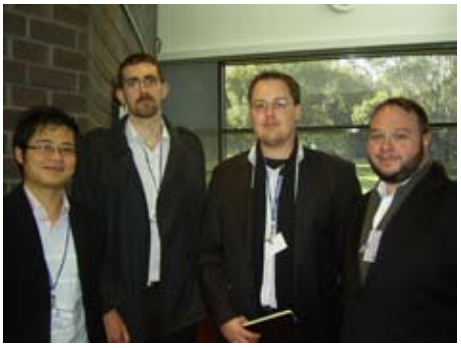
> "SPIDA - Secure Provenance of Identity Documents Analysis" - Ms Kylie Turville and UB's Dr Peter Vamplew.

Acting CIAO Director: Associate Professor David Yost

⇐ **Pictured (L to R):** Mr Desmond Lobo (UB), Mr Cameron Woolfe (IBM Executive-Ballarat) and Mr Robert Layton (UB)

Below (L to R): Workshop organisers Prof Josef Pieprzyk (Macquarie Univ) & A/Prof Paul Watters

Below (L to R): Workshop participants Dr Terry Tin (ANZ Bank), Westpac personnel Mr Ian Goldsmith, Mr Jackson McKinley and Mr Simon Brown



Below: Ms Amber Stabek receives her Best Paper Award from Mr Stephen McCombie

Dr Charlynn Miller

Staff Member Profile

Dr Charlynn Miller is the **Deputy Head of the Graduate School of Information Technology & Mathematical Sciences**, and has worked at the University of Ballarat since February 2003.

She is **Deputy Leader of the Virtual Reality & Simulation Laboratory**, and a Senior Lecturer within the School.

Dr Miller is also the Honours Coordinator for the School, and Coordinator for the School's Graduate Diploma of Advanced Computing.

She serves on the Academic Board of the University and the University Council, is **Chair of the Higher Education Learning & Teaching Committee**, and a member of UB's Higher Education Curriculum Committee.

Dr Miller is passionate about her work in **using emerging technologies to enhance learning**, and enjoys collaborating with colleagues in other disciplines.

She particularly enjoys working with students on projects and research initiatives which focus on **multi-disciplinary simulation learning within Virtual Worlds.**

Dr Miller attended **Virginia Commonwealth University** in the United States of America, where she gained a Bachelor of Science in Mathematical Sciences, a Post Baccalaureate Certificate in Human Resource Development, and a Master of Education in Adult Education.

She subsequently completed a **PhD in Higher Education** at the University of Virginia, USA.

Dr Miller has a **passion for education** and her key research interests are:
~ Emerging Technologies in Learning & Teaching
~ Podcasting
~ Virtual Worlds
~ Social Networking
~ Cyber-Bullying Prevention

She has been successful in obtaining **grants from a number of sources**, including most recently:

- Research Infrastructure Block Grant 2010: "Improving the Immersive Nature of the Virtual Reality Facility".

- Victorian Women's Benevolent Trust with Women's Health Grampians 2009: "Being Savvy in Cyberspace".

- School Focused Youth Service (Grampians Region) with Women's Health Grampians 2009: "Be Safe in Cyberspace".

- University of Ballarat, Higher Education Learning and Teaching Grant & Learning Leaders 2009: "'Hands On' Learning in Virtual Spaces".

She is currently **supervising five PhD students** on the following topics:

~ "An investigation of serious games and 3D simulation learning environments for the reinforcement of real world learning experiences" (Principal Supervisor).

~ "The Development of a Higher Education e-Learning Framework for Physical Education and Human Movement Students" (Principal Supervisor).

~ "Impact of structured decision support on decision making in online dispute resolution participants" (Associate Supervisor).

~ "How does Games Classification in Australia compare to International Classification and how relevant and transparent are the Australian Classification Levels" (Principal Supervisor).

~ "Understanding Victims of Identity Theft and Processes of Recovery" (Associate Supervisor).

To date she has **published sixteen journal papers, conference papers and book chapters.**

Dr Miller's **teaching focus** centres around Business Information Systems, Electronic Commerce, Emerging Technologies in Business, and IT Management.

She is a member of the Australian Computer Society, including the Women's Committee; Vic ICT for Women; and Phi Delta Kappa International.

Monash Visitor

Professor Frada Burstein

CIAO was pleased to host a recent visit from Professor Frada Burstein (pictured right), from the School of Information Technology at **Monash University** in Melbourne.

Professor Burstein's key research interests include **knowledge management**, intelligent decision support, cognitive aspects of information systems development and use, organisational knowledge and memory, and systems development.

She met with several CIAO personnel including long time associates Professor John Yearwood and Dr Andrew Stranieri, to talk about research areas of mutual interest.

While here Professor Burstein also presented a very interesting colloquium titled **"Information and Communication Technology for Effective Knowledge Management".**

Tracking copyright infringements in cyberspace

Researchers in CIAO's Internet Commerce Security Laboratory (ICSL) have created a program that will **detect copyright infringements in cyberspace.**

ICSL Director - **Associate Professor Paul Watters** (right) - says that a major risk to Australia's creative industries is the rise of illegal movie & music sharing over **peer-to peer (P2P) networks** like BitTorrent.

While there are many legitimate uses for BitTorrent, it has been used regularly to download and distribute copyright infringing material, such as movies, music and software.

As part of an ongoing project looking into **monitoring P2P network traffic**, ICSL researchers have developed a methodology to objectively answer some simple questions about copyright infringement.

They have been able to detect the **percentage of shared files that infringe copyright**, and what percentage of shared material belongs to different categories.

The project reports that 43.3% of BitTorrent downloads were movies, 29.1 per cent were TV shows and 16.5 per cent were music.

Using a sample of trackers, researchers discovered that a total of **117 million downloads** had been completed across more than one million torrents.

The top two files had been downloaded more than one million times each, and the third more than 500,000 times.

In summary, the project results indicate that approximately **89.9% of all torrents from the sample are infringing copyright,** both by the number of files and total downloads, excluding pornographic material.

Dr Watters believes this is the first time that someone has actually measured the results in this way.

The work was led by **Mr Robert Layton**, a PhD student studying at the ICSL, who focused on **automating the profiling of phishing attacks** through the use of **data mining** methods.

Mr Layton's work on automation has also extended to **authorship attribution of Twitter messages**, expert analysis feedback into clustering and now BitTorrent tracking.

Village Roadshow contributed to the funding of this project.

Detective Superintendent Brian Hay of **Queensland Police Fraud and Corporate Crime Group** said he was astounded by the extent of the findings.

He said the fact that such a large proportion of content was found to be in breach of copyright, provided an insight into an issue that had not previously been fully appreciated.

The findings of the report were presented at the **Second Cybercrime and Trustworthy Computer Workshop 2010** (see separate article on page 2).

Dr Paul Watters subsequently participated in a large number of media interviews.

Release of the project report led to more than **fifty international news articles** being written about the results of the study. The project has provided excellent publicity for ICSL and its important work at the University of Ballarat.

Modelling Aquifer Contamination

CIAO recently hosted a five-day **Modelling Aquifer Contamination Course** at the University of Ballarat.

International presenters at this event were **Professor Shaul Sorek** and **Dr Alexander Yakirevich** from the Department of Environmental Hydrology & Microbiology, Zuckerberg Institute for Water Sciences, **Ben-Gurion University**, Beer-Sheva, Israel.

Professor Sorek's presentations were titled:

> Lumped parameter models for flow and transport processes.

> Continuum Microscopic models for transport phenomena.

Dr Yakirevich presented on the topics:

> Flow in the subsurface.

> Solute transport in the subsurface.

> Techniques of parameter estimations.

> Modelling contaminant transport.

CIAO presenters were:

~ **Associate Professor Adil Bagirov:** Optimization methods of water distributions systems.

~ **Professor David Gao:** The canonical duality theory for solving general global optimization problems, and Dividing RECTangle method (DIRECT) for non-smooth optimization.

The course was organised by CIAO's **Dr Zari Dzalilov**, and provided a valuable forum for sharing research experiences and discussing future collaboration projects.

Right: Dr Alexander Yakirevich stands in front of his presentation

Below: Dr Andrew Stranieri makes a point to Professor Shaul Sorek

PhD Internship: Modelling Underwater Acoustics

PhD student Ms Liping Jin recently completed an **exciting industry internship** at the **Victorian Desalination Project (VDP)** in eastern Victoria.

Titled **"Modelling the underwater acoustics of desalination plants"**, the project's environmental objectives were to protect Wanthaggi township residents, coastal users and other nearby stakeholders from the plant's **noise emissions**.

This three-month internship was part of the **Australian Mathematical Sciences Institute (AMSI) Industry Internship Program,** and Ms Jin's Academic Mentor was UB's Associate Professor Adil Bagirov.

It involved Ms Jin working with industry partner **Marshall Day Acoustics Pty Ltd (MDA)**, who were appointed to survey and assess underwater noise at the VDP plant site.

Included in the project was an assessment of underwater noise impact on **marine divers and marine mammals.**

The VDP is located approximately six kilometres north-west of the **town of Wonthaggi**, along the **Bass coastline** of eastern Victoria, north of Tasmania. The VDP is in the vicinity of a former coal mine, on land previously used for farming.

The offshore area along this part of the coastline is a **shallow continential shelf** area with a water depth of less then 45 metres, within three kilometres of the VDP's seawater intake and outlet points.

Unlike deep water, shallow water is known to be **'relatively noisy'** in acoustic terms. **Ambient noise** in shallow water contains a mixture of shipping. industrial, wind and biological noise.

In addition, when the sea surface is smooth and calm, the water surface and the sea bed **form a sound channel** where sound is trapped by boundaries and propagates laterally very effectively.

Below: the project operating station on the boat.

Above: Ms Jin at the field survey with a team member.

The project team selected **ten measurement locations** around the VDP's seawater intake and outlet locations, at distances between 300m to 2.5 km.

The depth and distance from the shore were read from the boat's **sonar equipment**, and GPS directed the boat to each of the ten measurement locations.

Sound measurements were made using a **hydrophone** that was lowered into the water, and real time data recording was set up on the boat with the boat engine switched off.

The VDP's **twenty-six seawater lifting pumps** connecting the sea water intake heads by underground tunnel are the main offshore noise sources, when the VDP is in operation.

The pump noise propagates almost without any loss inside the hard tunnel to the intake head, and then propagates as a **cylindrical wave** to the surrounding sea water.

This internship provided a valuable opportunity for Ms Jin to contribute her **mathematical expertise** to a current State Government project, and make new contacts within local industry.

Below: Ms Jin and project team members preparing to depart on the boat.

Grants Awarded

ARC Discovery Grant 2010

Chief Investigator:
Dr Alex Kruger (right)

Topic: Stationarity & Regularity in Variational Analysis with Applications to Optimization

Partner Investigators:

- Professor Marco López Cerdá, University of Alicante, Spain
- Professor Michel Therá, University of Limoges, France
- Professor Jiri Outrata, Academy of Sciences, Czech Republic

Funding: $255,000 over three years

Colloquia @ UB

> *Dr David Cornforth*, CSIRO Energy Technology, CSIRO, Newcastle, NSW

Topic: Multiobjective Optimisation & Planning for the Integration of Renewable Energy

> *Professor Kate Smith-Miles* (pictured below), Head, School of Mathematical Sciences, Monash University, Melbourne

Topic: How data mining can reveal the secrets in your face - no more lying about your age!

Seminars @ UB

> *Dr Herbert Jelinek*, School of Community Health, Centre for Research in Complex Systems, Charles Sturt University

Topic: Medical Data -- what computer scientists need to know

> *Mr Olivier Lempert*, ecenta, AG, Germany

Topic: Typical project phases using ASAP methodology & project stakeholders in SAP Project

> *Professor Sergey Kuznetsov*, Russian Academy of Sciences, Moscow, Russia

Topic: Mathematical Methods in Surface Acoustic Wave Analysis

> *Mr Chris Lynton-Moll*, Chief Executive Officer, CAL2CAL Australia

Topic: Pencil, Paper or PDA?

Research Student Profile:

Mr Desmond Lobo

Mr Desmond Lobo (pictured above) commenced his PhD at the University of Ballarat in July 2007.

His research topic was "Rapid identification of rootkit infections using data mining", and he was supervised by Associate Professor Paul Watters (Principal) and Dr Xinwen Wu (Associate).

Rootkits are used to conceal the presence and/or activity of malicious software - known as malware - and to allow an attacker to take control of a computer system.

In this research, Desmond focused on rootkits that create hooks in the Microsoft Windows operating system in order to hide.

Unlike other malware identification strategies, the approach taken in his thesis involved developing a procedure that could be used to quickly identify the rootkits that have infected a machine, based on the hooks that have been detected in that machine.

Initially, only rootkits that construct inline function hooks were targeted.

Identifying these types of rootkits is a two-step process. Using an unsupervised clustering algorithm, Desmond first designed a technique that could effectively categorize a sample of rootkits into different families.

Next, using a logistic regression analysis for profiling these families, he was able to correctly identify at least one of the rootkits that had infected each of the machines that were tested.

Having had success with the collection of inline function hooking rootkits, he then proceeded to extend the sample set by including other types of rootkits, such as those that hook the import address table (IAT) and the system service descriptor table (SSDT).

With a greater variety of rootkits, Desmond was able to demonstrate that the iterative dichotomiser 3 (ID3) algorithm could be used to generate a decision tree for identifying the rootkit that had infected a machine.

A significant contribution of this research is that it provides clear evidence that the variants within a particular rootkit family have similar hooking patterns, and this suggests that these hooking patterns can be used to identify newly released variants from that family.

He concentrated exclusively on rootkits that attack Windows, because it is the dominant operating system in the world today.

Desmond identified some of the weaknesses in the Windows architecture which these rootkits exploit.

He concluded that Microsoft should take full advantage of Intel's four distinct privil-ege levels, in order to reduce the number of rootkit infections in the future.

Examination of his thesis was recently successfully completed.

Desmond is looking forward to graduating in December 2010, and we wish him the very best for the future.

« « « : » » »

Thesis Submission

Congratulations to the following PhD Student, who recently submitted her thesis for examination:

> Ms Armita Zarnegar (below)

Topic: "Gene Regulatory Network Discovery Using Heuristics"

Supervisors: Dr Peter Vamplew (Principal) and Dr Andrew Stranieri (Associate)

PhD: Confirmation of Candidature

Congratulations to the following PhD Students, who successfully completed their Confirmation of Candidature:

> Ms Nargiz Sultanova (below)

Topic: "Methods of nonsmooth nonconvex optimization & their application for optimization of electricity distribution systems"

Supervisors: Associate Professor Adil Bagirov (Principal) and Associate Professor David Yost (Associate)

> Ms Sona Taheri

Topic: "Bayesian Network Models based on Global Optimization"

Supervisors: Dr Musa Mammadov (Principal) and Associate Professor Adil Bagirov (Associate)

> Ms Alia Mari Al Nuaimat (below)

Topic: "Non-Smooth Optimization Algorithms for Solving Mixed Integer Non-Linear Programming Problems and their Application in Water Management"

Supervisors: A/Prof Adil Bagirov (Principal), A/Prof David Yost (Associate) and Dr Andrew Barton (Associate)

Publications

Books: Published

Gao, D.Y. & Motreanu, D. (editors) (2010) Handbook of Nonconvex Analysis & Applications, International Press of Boston.

Book Chapters: Accepted

Meredith, G. & Miller, C. (2010) The VSSC: A virtual beacon of self help for people who stutter, in Wankel, C. & Hinrichs, R. (Eds), 3D Virtual World Learning Handbook, Emerald Publishing.

Rogers, L., **Miller, C. & Firmin, S.** (2010) Evaluating the impact of a virtual emergency room simulation for learning, in Holt, D., Segrave, S., Cybulski, J. (Eds), Professional Education Using E-Simulations: Benefits of Blended Learning Design.

Book Chapters: Published

Venkatraman, S. (2010) A framework for ICT security policy management, Frameworks for ICT Policy: Government, Social & Legal Issues.

Journal Papers: Submitted/Accepted

Bagirov, A.M., Ganjehlou, A.N., **Ugon, J.** & Tor, A.H. (2010) A generalized subgradient method with piecewise linear subproblem, Dynamics of Continuous, Discrete and Impulsive Systems, Series B (A).

Bagirov, A.M. & Ugon, J. (2010) Codifferential method for minimizing nonsmooth DC functions, Journal of Global Optimization (A).

Li, G.Q., **Wu, Z.Y.** & Quan, J. (2010) A new local and global optimization method for mixed integer quadratic programming problems, Applied Mathematics and Computation (A).

Quan, J., Wu, Z.Y. & Bai, F.S. (2010) Global optimality conditions for some mixed integer programming problems, Dynamics of Continuous, Discrete & Impulsive Systems. Series B (A).

Rubinov, A.M., **Sukhorukova, N. & Ugon, J.** (2010) The choice of a similarity measure with respect to its sensitivity to outliers, Journal Dynamics of Continuous, Discrete & Impulsive Systems, Series B (A).

Sukhorukova, N. & Ugon, J. (2010) Characterization theorem for best linear spline approximation with free knots, Journal Dynamics of Continuous, Discrete & Impulsive Systems, Series B (A).

Wu, Z.Y., Li, D. & Zhang, L.S. (2010) Global descent methods for unconstrained global optimization, Journal of Global Optimization (A).

Zi, L., Yearwood, J. & Kelarev, A. (2010) An application of consensus clustering for DDoS attacks detection, Applications & Techniques in Information Security (A).

Journal Papers: Published

Bagirov, A., Clausen, C. & Kohler, M. (2010) An L2-boosting for estimation of a regression function, IEEE Transactions on Information Theory, Vol. 56, Issue 3, pp.1417-1429.

Fabian, M, Henrion, R., **Kruger, A.** & Outrata, J. (2010) Error bounds: necessary and sufficient conditions, Set-Valued and Variational Analysis, Vol.18, Issue 2, pp.121-149.

Gao, D.Y. & Ruan, N. (2010) Solutions to quadratic minimization problems with box and integer constraints, Journal of Global Optimization, Vol.47, Issue 3, pp.463-484.

Kelarev, A., Yearwood, J. & Watters, P. (2010) Internet Security Applications of Grobner-Shirshov Bases. Asian-European Journal of Mathematics, Vol.3, No.3, pp.435-442.

Kelarev, A., Yearwood, J., Watters, P., Wu, X., Abawajy, J. & Pan, L. (2010) Internet Security Applications of the Munn Rings, Semigroup Forum, Vol.81, No.1, pp.162-171.

Ruan, N., **Gao, D.Y.** & Jiao, Y. (2010) Canonical dual least square method for solving general nonlinear systems of quadratic equations, Computational Optimization and Applications, Vol.47, pp.335–347.

Van Ngai, H., **Kruger, A.** & Théra, M. (2010) Stability of error bounds for semi-infinite convex constraint systems, SIAM Journal on Optimization, Vol.20, Issue 4, pp.2080-2096.

Zhu, J., Zhou, J. & **Gao, D.** (2010) Global optimization by canonical dual function. Journal of Computational and Applied Mathematics, Vol.234, No.2, pp.538–544.

Conference Papers: Submitted/Accepted

Alazab, M. (2010) Forensic identification of hidden malware in the disk image, CTC 2010, 2nd Crime & Trustworthy Computing Workshop 2010, Ballarat, Jul 2010 (A).

Greenway, N. & **Miller, C.** (2010). Being savvy in cyberspace, Proceedings of the 6th Australian Women's Health Conference 2010, Australian Women's Health Network, Hobart, Tasmania (A).

Huda, S., Yearwood, J. & Borland, R. (2010) Smokers' characteristics and cluster based quitting rule discovery model for enhancement of Government Tobacco Control System, Pacific Asia Conference on Information Systems, PACIS 2010, Taiwan (A).

Lobo, D., Watters, P.A., Wu, X.W. & Sun, L. (2010) Windows Rootkits: Attacks and Countermeasures, CTC 2010, 2nd Crime & Trustworthy Computing Workshop 2010, Ballarat, Victoria, 19-20 Jul 2010 (A).

Meredith, G. (2010) The Debilitating "D" Word, ISAD 2010, International Stuttering Awareness Day Online Conference 2010 (A).

Stabek, A., Watters, P.A., & Layton, R. (2010) The Seven Scam Types: Mapping the Terrain of Cybercrime, CTC 2010, 2nd Crime & Trustworthy Computing Workshop 2010, Ballarat, Jul 2010 (A).

Turville, K., Yearwood, J. & Miller, C. (2010) Understanding Victims of Identity Theft: Preliminary Insights, CTC 2010, 2nd Crime & Trustworthy Computing Workshop 2010, Ballarat, Jul 2010 (A).

Conference Papers: Published

Dazeley, R., Yearwood, J.L., Kang, B.H. & **Kelarev, A.V.** (2010) Consensus Clustering & Supervised Classification for Profiling Phishing Emails in Internet Commerce Security, Knowledge Management & Acquisition for Smart Systems & Services, PKAW2010, Lecture Notes in Computer Science, 2011, Volume 6232, pp.235-246.

Pan, J.A., Winchester, D., Land, L. & **Watters, P.A.** (2010) Descriptive data mining on fraudulent online dating profiles, 18th European Conference on Information Systems 2010, Pretoria, South Africa.

Venkatraman, S. & Kulkarni, S. (2010) Risk-Based Neuro-Grid Architecture for Multimodal Biometrics, Innovations in Computing Sciences and Software Engineering, pp.51-56.

Centre for Informatics & Applied Optimization
Graduate School of Information Technology & Mathematical Sciences, University of Ballarat, Mt Helen Vic 3350
Email: e.matuschka@ballarat.edu.au ~ Tel: (+61) 3 5327 9949

Photograph by Elizabeth Matuschka: Spring blooms at Mt Helen Campus, University of Ballarat, Ballarat, Victoria, Australia