

SECAU

Security Research Centre.

Annual Report 2008.

(6 month Interim Report)

This report marks the first 6 months operation of the SECAU Security Research Centre. SECAU was officially opened on the 1st October 2008 by Professor Lynne Beazley, the WA Chief Scientist. The Security Research Centre is a Level II research centre currently based at the Mount Lawley Campus in the School of Computer and Information Science. Since the research centre was only opened on the 1st of October, this report represents a 6 month interim report, detailing the achievements of the first 6 months of operation (October 2008 – March 2009).

The overarching strategy for the first 6 months of operation was to bring together the various elements of security research across numerous schools and boundaries in order to form a research continuum that incorporated physical and digital security. The resulting holistic approach now means that SECAU has a scope that investigates security issues from technology through to human factors. The principle areas of focus are Computer and Digital Forensics, Network and Wireless Security, Information Warfare, Physical Security, Risk management, Surveillance/CCTV, and Critical Infrastructure Protection.

The centre has aimed to become the peak, end to end, security research group in Australia. Unlike other research groups that might purport to occupy the same research space, SECAU operates as a “solutions-based” research enterprise that engages with and partners alongside Australia’s foremost State and federal security organisations, enforcement services and private security environments.



SECAU Group Members

SECAU Consists of the following members:

Professor Bill Hutchinson - Director (IBM Chair in Information Security)
Associate Professor Craig Valli – Head of School (School of Computer and Information Science)
David Cook – Manager SECAU

Professor Nara Srinivasan - Professor of Security and Risk
Professor Murray Lampard APM – Professor of Security
Dr David Brooks
Dr Patricia Williams
Dr Andrew Woodward
Dr Geoff Swan
Bill Bailey
Jeff Corkill
Peter Hannay
Chris Bolan
Patryk Szewczyk
Glen Thompson
Brett Turner

Special Interest Group members:

The SECAU Security Research Centre has built up a membership of more than 540 security stakeholders who have an informal association with the research centre by means of regular monthly Special Interest Group meetings and presentations. The membership includes the leading members from all of the Security-related partnerships, associations and agencies that have a research or interest-based relationship with SECAU and its various research directions.

Grants: GovCERT allocated \$5000 in funds for data derived from Hard Drive studies looking at Remnant Data.

Publications:

Books:

1. Valli, C. (2009) Building a Digital Forensic Laboratory: Establishing and managing a Successful Facility, Butterworth-Heinemann

Journals:

1. El-Moussa, F. and A. Jones (2008). "A Malware Analysis: The Art of Detecting Malicious Activities." Journal of Information Warfare 7(3): pp23-34.
2. Jones, A. (2008). "Catching the Malicious Insider." Information Security Technical Report 13(4): pp220-2
3. Jones, A., C. Valli, et al. (2008). "The 2007 Analysis of Information Remaining on Disks offered for sale on the second hand market." Journal of Digital Forensics, Security and Law 3(1): pp5-24.
4. Jones, A., C. Valli, et al. (2008). "Analysis of Information Remaining on Hand Held Devices for Sale on the Second Hand Market." The Journal of Digital Forensics, Security and Law 3(2): pp55-70.
5. McEniery, D. and A. Woodward (2008). "Australian Defense Force Policy and the use of WPA2 as a security option for deployment of 802.11 wireless devices in the field." Journal of Information Warfare 7(3): pp35-54.
6. Williams, P. A. H. (2008). "In a 'trusting' environment, everyone is responsible for information security." Information Security Technical Report 13(4): pp207-215.
7. Williams, P. A. H. (2008). "When trust defies common security sense." Health Informatics Journal 14(3): pp211-221.
8. Williams, P. A. H. (2008). "A Practical Application of CMM to Medical Security Capability. ." Information Management and Computer Security 16(1): pp58-73.

Conference Presentations and Refereed Papers:

1. Al-Hajri, M. (2008). An overview of Mobile Embedded Memory and Forensics Methodology. the 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University Perth WA, SECAU Security Research Centre: pp 19-29.
2. Al-Hajri, M. and K. Sansurooah (2008). iPhone Forensics Methodology and Tools. The 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University WA, SECAU Security Research Centre: pp 4-18.
3. Ami-Narh, J. and P. A. H. Williams (2008). Digital forensics and the legal system: A dilemma of our times. the 6th Australian Digital Forensics Conference. C. V. a. A. Woodward. Edith Cowan University, Perth, WA., C. Valli and A. Woodward: pp30-40.

4. Bailey, W. and A. McGill (2008). Freedom Fighters or Terrorists by another Name? the 1st Australian Security and Intelligence Conference. C. V. a. D. Brooks. Edith Cowan University, Mount Lawley Campus WA, SECAU Security Research Centre: pp84 - 92.
5. Boeing, A. (2008). Survey and future trends of efficient cryptographic function implementations on GPGPUs. The 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University WA, SECAU Security Research Centre: pp59-69.
6. Boeing, A., M. Masek, et al. (2008). Protecting Critical Infrastructure with Games Technology. The 9th Australian Information Warfare and Security Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth western Australia, SECAU Security Research Centre: pp27 - 34.
7. Bolan, C. (2008). A Review of the Electronic Product Code Standards for RFID Technology. Proceedings of the Seventh International Network Conference. P. S. D. a. S. M. Furnell. Plymouth. UK, Centre for Information Security and Network Research: pp 171-180.
8. Bolan, C. (2008). RFID Communications - Who is Listening? The 6th Australian Information Security Management Conference. C. V. a. A. Woodward. Edith Cowan University, Mount Lawley Campus, Western Australia, SECAU Security Research Centre: pp19-28.
9. Corkill, J. (2008). Professional Intelligence Judgement Artistry. the 1st Australian Security and Intelligence Conference. C. V. a. D. Brooks. Edith Cowan University Mount Lawley Campus, SECAU Security Research Centre, Edith Cowan University WA: pp17 -25.
10. East, A. and W. Bailey (2008). Australia's Oil Refining Industry - Importance, Threats and Emergency Response. the 1st Australian Security and Intelligence Conference. C. V. a. D. Brooks. Edith Cowan University Mount Lawley Campus ECU WA, SECAU Security Research Centre: pp37 - 43.
11. Griffiths, M. and W. Bailey (2008). Aviation Infrastructure Protection: Threats Contingency Plans and the Importance of Networks. the 1st Australian Security and Intelligence Conference. C. V. a. D. Brooks. Edith Cowan University Mount Lawley Campus WA, SECAU Security Research Centre: pp44-55.
12. Hannay, P. (2008). Forensic Acquisition and Analysis of the TomTom One Satellite Navigation Unit. the 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University Perth WA, SECAU Security Research Centre: pp78-81.
13. Hannay, P. and A. Woodward (2008). Cold boot memory acquisition: An investigation into memory freezing and data retention claims. The 2008 International Conference on Security and Management S. A. Hamid R. Arabnia, and Mark Bedworth. Monte Carlo Resort Las Vegas USA, CSREA Press, U.S.A.: pp620-622.
14. Helala, M., S. Furnell, et al. (2008). Evaluating the usability impacts of security interface adjustments in Word 2007. The 6th Australian Information Security Management Conference. C. V. a. A. Woodward. Edith Cowan University, Mount Lawley Campus, Perth Western Australia, SECAU Security Research Centre: pp48 - 55.

15. Hutchinson, W. (2008). The Ethics of Information Operations. The AiCE 2008 Fifth Australian Institute of Computer Ethics Conference. M. Warren. Deakin University, Burwood, Victoria, Australia, School of Information Systems Deakin University, Burwood, Victoria, Australia: pp63-67.
16. Hutchinson, W. (2008). Propaganda Dilemmas for Environmental Security. Proceedings of the 7th European Conference on Information Warfare and Security. Dan Remenyi. University of Plymouth, University of Plymouth: pp103-110.
17. Hutchinson, W. (2008). Media, government and manipulation: the cases of the two Gulf Wars. The 9th Australian Information Warfare and Security Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth western Australia, SECAU Security Research Centre, ECU: pp35-40.
18. Jones, A. and C. Colwill (2008). Dealing with the Malicious Insider. Proceedings of 6th Australian Information Security Management Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth WA, SECAU Security Research Centre ECU: pp87 - 100.
19. Jones, A. and I. Sutherland (2008). Industrial Espionage from Residual Data: Risks and Countermeasures. 6th Australian Digital Forensics Conference C. V. a. A. Woodward. Edith Cowan University, Perth, Western Australia, SECAU Security Research Centre: pp165-170.
20. Jurcic, D. (2008). Modern Society as Risk Society: Implications of Modernity on Private Security. the 1st Australian Intelligence and Security Conference. C. V. a. D. Brooks. Edith Cowan University - Mt Lawley Campus WA, SECAU Security Research Centre: pp56 - 60.
21. Kaur, M. and A. Jones (2008). Security Metrics - A Critical Analysis of Current Methods. The 9th Australian Information Warfare and Security Conference. C. V. a. A. Woodward. Edith Cowan University, perth, Western Australia, SECAU Security Research Centre: pp41-47.
22. Kevans, P. and W. Bailey (2008). A New definition of Piracy in South East Asia required? the 1st Australian Security and Intelligence Conference. Edith Cowan University, Mt Lawley Campus, SECAU Security Research Centre, ECU WA: pp61-75.
23. Pasupatheswaran, S. (2008). Data recovery from PalmmsgV001. the 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University Perth WA, SECAU Security Research Centre.
24. Pasupatheswaran, S. (2008). Email 'Message-IDs' helpful for forensic analysis? Proceedings of the 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University Perth WA, SECAU Security Research Centre: pp126-139.
25. Smart, J., K. Tedeschi, et al. (2008). Subverting National Internet Censors: An Investigation into Existing Tools and Techniques. the 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University WA, SECAU Security Research Centre: pp158-164.
26. Swanson, I. (2008). Malware, Viruses and Log Visualisation. the 6th Australian Digital Forensics Conference, Edith Cowan University Perth WA, SECAU Security Research Centre.

27. Szewczyk, P. and M. Brand (2008). Malware Detection and Removal: an examination of personal ant-virus software. The 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University WA, SECAU Security Research Centre.
28. Tank, R. and P. A. H. Williams (2008). The impact of U3 devices on forensic analysis. the 6th Australian Digital Forensics Conference, . C. V. a. A. Woodward. Edith Cowan University, Perth, WA. , SECAU Security Research Centre: pp197-203.
29. Turner, B. and A. Woodward (2008). Network security isn't all fun and games: an analysis of information transmitted whilst playing Team Fortress 2. The 6th Australian Security Management Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth WA, SECAU Security Research Centre: pp138-144.
30. Turner, B. and A. Woodward (2008). Securing a Wireless network with EAP-TLS: perception and realities of its implementation. The 6th Australian Information Security Management Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth WA, SECAU Security Research Centre ECU: pp130-137.
31. Valli, C. and M. Brand (2008). The Malware Analysis Body of Knowledge (MABOK). Proceedings of the 6th Australian Digital Forensics Conference. V. a. Woodward. Edith Cowan University Perth WA, SECAU Security Research Centre: pp70-77.
32. Valli, C. and A. Jones (2008). A Study into the Forensic Recoverability of Data from 2nd Hand Blackberry Devices: World-Class Security, Foiled by Humans. The 2008 International Conference on Security and Management (SAM'08). S. A. Hamid R. Arabnia, and Mark Bedworth. Monte Carlo Resort Las Vegas USA, CSREA Press, U.S.A.: pp604-607.
33. Valli, C. and A. Woodward (2008). The 2008 Australian study of remnant data contained on 2nd hand hard disks: the saga continues. The 6th Australian Digital Forensics Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus WA, SECAU Security Research Centre ECU: pp211-214.
34. Williams, P. A. H. (2008). Virtual environments support insider security violations. the 6th Australian Digital Forensics Conference, . C. V. a. A. Woodward. Edith Cowan University, Perth, WA., SECAU Security Research Centre: pp171-178.
35. Williams, P. A. H. (2008). Can an Adapted Clinical Governance Model be used to Improve Medical Information Security? the 7th European Conference on Information Warfare and Security. D. Remenyi. Plymouth UK, Academic Publishing Limited, Reading: pp219-228.
36. Williams, P. A. H. (2008). Is There an Ideal Forensic Process? The 2008 International Conference on Security and Management S. A. Hamid R. Arabnia, and Mark Bedworth. Monte Carlo Resort Las Vegas USA, CSREA Press, U.S.A.: pp598-603
37. Williams, P. A. H. and R. Mathew (2008). Can intrusion detection implementation be adapted to end-user capabilities? The 6th Australian Information Security Management Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth Western Australia, SECAU Security Research Centre: pp145-154.

38. Williams, P. A. H. and C. Valli (2008). Trust me. I am a doctor. Your records are safe... The 6th Australian Information Security Management Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth Western Australia, SECAU Security Research Centre: pp 155-162.
39. Woodward, A. and C. Valli (2008). Issues common to Australian critical infrastructure providers SCADA networks discovered through computer and network vulnerability analysis. . The 6th Australian Digital Forensics Conference. C. V. a. A. Woodward. Edith Cowan University Mount Lawley Campus Perth WA, SECAU Security Research Centre: pp204-208.
40. Woodward, A. (2008). What Artefacts do Current BitTorrent Clients Leave Behind? . The 2008 International Conference on Security and Management (SAM'08). S. A. Hamid R. Arabnia, and Mark Bedworth. Monte Carlo Resort Las Vegas USA, CSREA Press, U.S.A.: pp608-613.
41. Woodward, A. and P. Hannay (2008). Forensic implications of using the firewire memory exploit with Microsoft Windows XP. The 2008 International Conference on Security and Management (SAM'08). S. A. Hamid R. Arabnia, and Mark Bedworth. Monte Carlo Resort Las Vegas USA, CSREA Press, U.S.A.: pp593-597.

HDR Load:

Usman Farooq	PhD Candidate
Krishnun Sansurooah	DIT Candidate
Peter Hannay	PhD Candidate
Chris Bolan	PhD Candidate
Patryk Szewczyk	PhD Candidate
Sunsern Limwiriyakul	DIT Candidate
Marwan Al-Zarouni	DIT Candidate
Glen Thompson	PhD Candidate
Nattakant Uttakrit	DIT Candidate
David Shaw	PhD Candidate
Peter James	DIT Candidate
Brett Turner	Master of Science (Comp Security)
Murray Brand	Master of Science (Comp Security)
Peter James	DIT Candidate

HDR Completions:

Edwin Leigh Armistead Doctor of Philosophy
'The Information Strategy Requirements of the Unites States Government from 2004 Onwards'

Key Visitors and Collaborators:

International

Dr Craig Donald, CCTV expert from South Africa, was a keynote speaker at the SECAU Security Congress organised and hosted by the SECAU Security Research Centre. 1st-3rd December 2008. He spoke on the importance of human factors in the effective widespread use of CCTV technology.

Professor Andy Jones, British Telecoms, was a keynote speaker at the SECAU Security Congress organised and hosted by the SECAU Security Research Centre. 1st-3rd December 2008.

Professor Glenn Dardick, Assistant Professor of Information Systems at Longwood, was a keynote speaker at the SECAU Security Congress organised and hosted by the SECAU Security Research Centre. 1st-3rd December 2008. He spoke on the importance of understanding cyber forensic evidence.

Mr David Mitchell, Mr Ronen Nadir and Mr Ziv Barak, from Israel spoke at the 22nd October Special Interest Group on Unmanned Airborne Vehicles. The Presentation focussed on new advances in UAV technology, as well as highlighting security tactics and spatial planning implications.

SECAU are leading contributors in an international research program to investigate the presence of sensitive information on second hand computers. The collaboration between SECAU, the University of Glamorgan in Wales, Longwood university in the United States, and British Telecoms (BT) in the UK is a longitudinal study into hard drives purchased in second hand condition from the public domain in the UK, US, Europe and Australia.

National

Mr Paul O'Sullivan, Director-General ASIO visited ECU on the 6th November and spoke on the topic of "*The Australian Security Environment and the Importance of Security and Research*". The public lecture drew interest from security students and academic staff as it highlighted the urgent need for academic excellence in the nation's security, and gave comment on new areas of focus for security teaching and research.

Mr David Healey, Director of GovCERT, was a keynote speaker at the SECAU Security Congress organised and hosted by the SECAU Security Research Centre. 1st-3rd December 2008. He outlined the new Australian directions in regards to Computer Emergency responses and outlines the nation's e-security policy directions.

SIMPLE: SECAU in conjunction with the Australian Federal Police and the WA Police are developing a forensics device that assists in the detection of Child Pornography images on computers. Dubbed SIMPLE (Simple Image Preview Live Environment) – the forensic program enables officers in the field to examine images on computers in a forensically clean manner. The device does not write any information to a computer and computers taken as evidence remain a forensically clean piece of evidence if required for prosecution.

Local

Professor Lyn Beazley, The WA Chief Scientist, opened the SECAU Security Research Centre on 1st October 2008. The event was attended by 100 guests and at which Professor Beazley acknowledged the critical work being undertaken by ECU in the area of Security Research.

Professor Kerran Campbell, Associate Professor, spoke at the 9th April SIG Special Interest Group on the topic of “Technology in Aviation Security”. He illustrated the latest security issues at Airports and highlighted future areas for research into mitigating potential threats.

Dr Anne Aly, spoke at the 25th November Special Interest Group on the topic of “Modern profiling for a counter-terrorism response”. Dr Aly gave an insight into Muslim cultural and social tendencies that impact on terrorist profiling within the Australian Counter-terrorism context.

SOHO: Lecturers Patryk Szewczyk and Brett Turner have (in conjunction with HoS Associate Professor Craig Valli) been developing a Small Office / Home Office website that teaches security focused computer literacy to home office users and the general public. The SOHO project also collects survey material to collect data about security cyber risks in the home and on personal laptops.

Community Engagement Activities and Linkages.

Special Interest Group Presentations.

The research centre has been active in establishing a robust membership of 540 local and national security stakeholders who have supported a range of Special Interest Group meetings and forums. These presentations have been held every month at Edith Cowan University and have been shared between the Mt Lawley and Joondalup Campuses. The SIG membership is a rich source of stakeholders and security actors ranging from security professionals, associations, student groups through to agency representatives from security and policing agencies at both state and federal levels.

Counter Terrorism Roundtable

The research centre has held the first of several counter-terrorism (CT) roundtable forums to develop research collaborations within the university. The Roundtables have been chaired by Professor Bill Hutchinson. By employing a cross-disciplinary approach the centre hopes to develop a range of unique partnerships that draw together science and technology, law and governance and human and social factors. SECAU recognises and promotes the notion that CT requires multiple agency in order to create these distinctive research directions.

AISA

SECAU has forged a strong relationship with the Australian Information Security Association. Associate Professor Craig Valli is a foundation member and sits on the AISA Board in WA. SECAU academic staff have contributed to the association’s engagement and public presentations at their monthly meetings in the Ernst and young facilities in the Perth CBD.

ANZFSS

SECAU has maintained a strong relationship with the Australia and New Zealand Forensic Science Society and Associate Professor Craig Valli is an active committee member on the state executive committee. ANZFSS have worked closely with SECAU on a range of security and forensic initiatives.

ASIS

SECAU has renewed a strong relationship with ASIS and Professor Bill Hutchinson is the Chairman of the WA Chapter. ASIS and SECAU are working together to develop a nucleus of security practitioners within the WA context. ASIS meetings coincide with SECAU Special Interest Group meeting days in order to maximise networking and collaborative advantages amongst a range of extremely busy practitioners and security professionals.

Future Plans and Directions

SECAU has developed a number of major grant proposals and funding applications which will greatly increase its research profile. Many of these applications for funding fall outside the normal structure of ARC grant planning and instead rely on the close relationships that SECAU has developed with key government agencies such as ASIO, DSD, GovCERT, the Attorney Generals Department, the AFP, and the Western Australian Police.

Much of the research activity is of a sensitive nature and reinforces SECAU's position as one of Australia's leading security research facilities. In 6 months SECAU has already established itself as a leader in the area of SCADA research, Honeypots, GPS Forensics, Remnant data, Disaster Victim research, Child Pornography Forensics and Wireless Security.

Future projects that will develop in the next 6 months include the CISL Laboratories (Critical Infrastructure and Security laboratories) which SECAU will launch in the next 30 days. These will further develop the Research Centre's capabilities in the area of CNVA (Computer Network Vulnerability Assessments), Red Teaming, and Penetration Testing. The CISL Laboratories will give ECU Australia's only Critical Infrastructure Test facility, with the next closest facility being located in Idaho in the United States. Given the high strategic importance given to CIP (Critical Infrastructure Protection) – the CISL laboratories will mark a substantial leap forward in collaborative security research. It is expected to draw research collaborations from all of the major power, water and energy providers across Australia. In conjunction with GovCERT and the Federal Attorney Generals Department, the CISL laboratories will develop the next generation of CIP for Australia.

In the next 12 – 18 months SECAU will develop a number of other research projects including CCTV, Port security, Biometric Device Analysis, and Counter Terrorism.

Date of Next formal review.

This Research Centre report is only a 6 month interim report, as the centre has yet to complete a full cycle of 12 months. The SECAU Security Research Centre will review its performance at the end of its first 12 months after October 2009.