School of Engineering, Computing and Applied Mathematics

Security Research Group

- Protecting people, information and infrastructure.

UNIVERSITY of ABERTAY DUNDEE

Personnel and expertise

Mr Andy Sapeluk	*– biometrics*
Dr Ian Ferguson (SRG coordinator)	*– digital forensics*
Dr Les Ball	*– intelligence and security informatics, biometrics*
Dr Natalie Coull	*– ethical hacking*
Dr Jackie Archibald	*– usable security*
Dr Matthew Craven	*– cryptography*
Mr Colin McLean	*– ethical hacking*
Dr Allan MacLeod	*– penetration testing, mobile and sensor networks*
Mr Malcolm Mactavish	*– web application security*
Dr Suheyl Ozveren	*– smart grids and power systems*
Dr Colin Cartwright	*– human factors and image analysis*
Dr Petra Leimich	*– database security*
Dr Geoff Lund	*– mobile systems*
Dr Andrea Szymkowiak	*– biometrics*
Dr Naghmeh Moradpoor	*– network security*
Mr Gavin Hales	*– PhD student – forensic visualization*
Ms. Lynsay Shepherd	*– PhD student – usable security*
Mr Scott Mitchell	*– PhD student – countermeasures to digital piracy*
Mr Ethan Bayne	*- PhD student – Digital Forensics Rapid Analysis Development*

All the above can be contacted via email by using <first initial>.<lastname>@abertay.ac.uk - 01382 308 600

cybersecurity.abertay.ac.uk

Interests

The Security Research Group (SRG) at Abertay are pursuing several themes in the security area:

Usable Security – developing new UI metaphors for security and embedding them in security design methodology thus putting people at the heart of system security.

Biometrics – multimodal border control, biometric passwords.

Digital Forensics - reconstruction of web browsing, email and social networking activity through the analysis of digital forensic artefacts.

Security/Digital Forensic Visualization – investigating the use of interactive graphical data exploration to aid investigation, reconstruction and incident response.

Intelligence Systems – Open Source Intelligence and counterterrorism.

Smartgrid Security - critical infrastructure protection.

Ubiquitous Security – protecting the cloud, mCommerce and mobile computing.

Recent Successes

- The work of SRG has been supported by the competitive award of two SICSA (Scottish Informatics and Computer Science Alliance[1]) PhD studentships.
- Two KTP awards with NCR (rated 'excellent' and 'very good') on securing ATMs against malware and hacking.
- *Biometric keyboard* - Two patents have been filed on the use of keystroke dynamics as a biometric identifier, a project supported by a grant from the Carnegie Trust. The work is evolving into whether a “stress” typing signature can also be identified.
- Members of the SRG are engaged in professional practice, consultancy and case work (expert witness).
- Professional Development Course in Ethical Hacking.

Current and Recent Projects

KLipCorp – Forensic Investigation of IPR infringement

1 www.sicsa.ac.uk

via streaming IPTV (commercial project/SFC Innovation Voucher)

This project has lead to the development and deployment of techniques for the protection of digital TV from IP-based video piracy. By reverse engineering pirate video streams, the P2P distribution network can be investigated. A follow-on project investigating potential countermeasures is about to get under way.

Dr A. MacLeod/Dr R.I. Ferguson

InSight - Digital forensic visualization – SICSA funded PhD studentship

- Whilst much research effort has been put into tools for preserving and searching the large volumes of unstructured data that characterise digital forensic investigations, there is a paucity of tools for analysis and reconstruction. InSight aims to use Data Visualization and 3D graphical techniques to enable interactive data exploration of evidence.

Dr R.I. Ferguson/Mr G. Hales

Usable Security – SICSA funded PhD studentship

Recent research suggests that because security within computer systems can be cumbersome and in places difficult, people take short cuts and end-up making insecure interactions. Current work focuses on whether the use of Affective Feedback may encourage the user to interact more securely and thus not make security compromises.

Dr J. Archibald/Ms L. Shepherd

CPD Courses for EPCC

- training in penetration testing has been carried out for commercial clients including the Edinburgh Parallel Computer Centre

Mr C. McLean

Upbeet – Social Network Analysis

UPBEET is a collaborative project between the University and Dundee based charities. The project aimed at improving social and community links for isolated young people in the area, via mobile and other devices. The project has evaluated the publicly available social networks in terms of their privacy and security. Future developments will see the project make use of social networking design patterns, but will ensure data privacy by creating and hosting the service.

Ms D. Carmichael

mCommerce

Authenticating the identity of a mobile user is now a key requirement of many apps. We are building new models of authentication more appopriate for this task. Current work is focused on biometrics and recognising the behaviour of the individual.

Dr G. Lund

Mathematical Underpinnings of Security

Work on mathematical aspects of security builds on a background in cryptography, mathematical modelling, discrete mathematics and combinatorial optimisation. Publications in the area include work on evolutionary algorithms for the solution of cryptographic problems posed over algebras and groups and, related to this work on analysis of algorithms, parameter optimisation and statistical structures of spaces.

Current interests include probabilistic attacks on cryptosystems that have been recently proposed and the application of if this in the broader area of cyber-security. Interesting blue-sky research projects in Risk management in computer security (quantification of risk in a computer system via a mathematical model); and Mathematical sociology (quantification of the human factors) in computer security are also planned.

Dr M. Craven

SQLlite - Forensic analysis of phone,browser, email and other artefacts

Many web browsers and email clients store information locally in underlying databases, particularly SQLite. This also applies to mobile phone operating systems such as Android. This suite of projects investigates what information is stored where and how it can be recovered even after being deleted.

Dr P. Leimich

Reverse authentication

Users are constantly required to authenticate themselves and prove their identity online or while conducting financial transactions. To take advantage of our reliance on technology, malicious hackers are using increasingly sophisticated methods to steal the data that could help them authenticate themselves as their victim. Some of these methods include the malicious hacker posing as the business and stealing their credentials via a telephone call, phishing email or fake website. It can be very difficult for users to differentiate the genuine business communications from the malicious phishing ones.

Reverse (or two-way) authentication is required to provide a method of business authentication to the user, so that they can have confidence that their communication is with a genuine business and not a malicious hacker. This two way authentication could be implemented in a number of different ways, from a shared password in an existing business-to-customer relationship to a 3rd party tool that is able to verify that a communication has come from a valid and trusted source.

Dr N. Coull

Penetration Testing

Penetration testing services have been provided by students to Univ. of Edinburgh and Univ. of St Andrews

NCR Dundee - Securing ATMs against malware and hacking (commercial project/KTP)

- investigated means of hardening ATMs against attack and developed countermeasures against a range of threats/attack modes.

Mr C. McLean

Biological metaphors for combating 'botnets

- Viewing 'botnet infections through the mathematics of epidemiology leads to the idea of artificial immune systems as a defence/healing mechanism. This project is seeking to establish the feasibility of such an approach.

Dr N. Coull

Biometrics

- developing and evaluating a biometrics scanner that can operate as a multi-modal system by acquiring and analysing physiological and behavioural biometric traits in real-time. For example merging face, voice and gait data. We are also evaluating the effect of using a Kinect camera to analyse gait data under normal conditions and under conditions of loading to simulate the posture and gait of a potential suicide bomber.

Dr L. Ball/Mr A Sapeluk

Forensic image triage – (SIPR/Tayside Police)

- Investigated means by which the processing of digital forensics cases can be accelerated through the application of computer vision techniques.

Ferguson, Ball, Sapeluk

Cyber Intelligence

High-profile terrorist attacks in the new Millennium have made counter-terrorism a priority for many governments. The abundance of open source intelligence available after the 9/11/2001 attack, for example, enabled a comprehensive analysis of that terrorist network. The opportunity, thus, is to collect valuable and cost-effective information during the pre-attack phase to aid in the prevention of such atrocities in the future. Social network analysis as a key tool for this type of intelligence analysis, with emphasis on the automated extraction of data relevant to the structural organisation of its actors and the attributes of their relationships in the network by using data and text mining techniques on open sources. These processes are viewed as a layer that could complement and help to populate a terrorist behavioural activity model, where the recognition of pre-incident indicators are linked to the likelihood of terrorist events.

Dr L. Ball

Empowerment through computing

- Allowing people access to information, data, services and devices they would not normally be able to use. The reason for the lack of access can be far reaching, everything from disability to simple lack of knowledge and experience, and can include both expert and non-expert users. This area of research includes aspects of visualisation, modelling, security, HCI and user centred design. Current work includes an EU funded project (iAge) investigating user centred design of mobile and tablet applications for older and disabled users whilst previous projects have looked at the development of an interactive visualisation platform which uses modelling and real time simulation to aid the comprehension of complex information, increase stakeholder interaction and provide real-time decision impact assessment. This platform could be applied to security.

Dr J. Isaacs

Digital Forensic Rapid Analysis Development

The current generation of digital forensic tools have difficulty in dissecting large volumes of digital evidence and displaying results in a readable format to the investigator. This research aims to investigate methods of advancing digital forensic tools with parallelism and visualisation to enable quick analysis and clear presentation of evidence.

Dissemination

Some Recent Publications

Ferguson, R.I., Ball, L. & Sapeluk, A., *SafeList: A Digital Forensic Triage Assistant*, Proc. of Cyberforensics 2011, Univ. Strathclyde, June 2011

Lowman, S. and Ferguson, R.I., *Web History Visualization for Forensic Investigations*, Proc. of Cyberforensics 2011, Univ. Strathclyde, June 2011

A.D. Irons, P. Stephens, R.I. Ferguson, Digital Investigation as a distinct discipline: A pedagogic perspective, Digital Investigation, Volume 6, Issues 1-2, Pages 1-92 (September 2009)

Hales, G., Ferguson, R.I., Archibald, J., *On the use of data visualization techniques to support digital forensic analysis: A survey of current approaches*, Proc. of Cyberforensics 2012, University of East London, May 2012

Walker, N., Coull, N., Ferguson, R.I. and Milne, A. *On the use of Design Patterns to Capture Aspects of Memory Corruption Vulnerabilities*, CyberPatterns 2012, in Proc. The First International Workshop on Cyber Patterns: Unifying Design Patterns with Security, Attack and Forensic Patterns (CyberPatterns2012) 9-10

July 2012, Abingdon, Oxfordshire, UK, 2012

Ferguson, R.I., Leimich, P. and Bagley, R., *On the digital forensic analysis of the Firefox browser via recovery of SQLite artefacts from unallocated space*, CFET2012, Canterbury, Kent, UK, 2012

Ball, L. Ewan, G. Coull, N. (2012) U*ndermining - Social Engineering using Open Source Intelligence Gathering* 4th International Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management. October 2012.

Ball L. (in press) Automating Social Network Analysis: A Power Tool for Counter-Terrorism, Security Journal.

Dowman, M., Szymkowiak A, Hapca S, Coull N and Ball L. A biometric system for identifying individuals and consideration of their emotional signatures from keystroke metrics, submitted to PNAS.

Shepherd, L., Archibald, J.M. & Ferguson, R.I., "Aiding end-user awareness of risky behaviour in relation to Computer Security: a review", awaiting publication in "Neuroscience perspectives on Security: Technology, Detection, and Decision Making" a special issue of "Frontiers in Neuroscience"

Shepherd, L., Archibald, J.M. & Ferguson, R.I., Perception of risky security behaviour by users: survey of current approaches, HCI International 2013 (accepted for publication)

Dowman M, Szymkowiak A, Coull N, Ball L. "Profiling user behaviour to reveal computer misuse".3rd Annual SIPR conference, 2009

Craven, M. ,An Evolutionary Algorithm for the Solution of Two-Variable Word Equations in Partially Commutative Groups, Studies in Computational Intelligence 153, Springer (2008), 3—19.

Craven, M. & Jimbo, H.C., A Kolmogorov-Type Stability Measure for Evolutionary Algorithms, in "EvoCOP 2011" (P. Merz et al., eds.), LNCS 6622, Springer (2011), 26—37.

Craven, M. & Jimbo, H.C., An Evolutionary Algorithm Solution of the Multiple Conjugacy Search Problem in Partially Commutative Groups with Applications, Groups, Complexity and Cryptology 4 (2012), 135-165.

Teaching

The SRG supports the teaching of several undergraduate and postgraduate programmes:

- BSc Ethical Hacking and Countermeasures
- BSc Digital Forensics

- MSc Ethical Hacking and Computer Security
- MSc Intelligence and Security Informatics
- MSc Digital Forensics

Media, Public Engagement and Outreach

Members of the SRG have recently contributed interviews on cybersecurity related matters to BBC Reporting Scotland, BBC Radio Scotland, BBC Radio London, BBC Radio Wales, The American Forces Network and the Dundee Courier.

- SecuriTay – Student-organised CyberSecurity Conference
- Holyrood Magazine - "Tricking, not hacking – protecting public sector IT against social engineering" - Gavin Ewan and Colin McLean, http://www.holyrood.com/2012/06/whats-your-weakness/
- BCS Security, Data and Privacy., "The innocent hillwalker", Les Ball and Natalie Coull http://www.bcs.org/content/conWebDoc/49687
- Dr Ferguson gave the invited keynote address at the 3rd Int'l Conf. on Mobile Security (MobiSec 2011) in Aalborg, Denmark
- Dr Ball was an invited contributor to a Video Round Table on National Security. Other contributors are leading government advisors and software companies, Nov 7th, London, 2011.
- Dr Ball gave a presentation at the International Crime and Intelligence Analysis Conference, Manchester, Nov 3-4, 2011
- Colin Maclean - Ethical Hacking presentation at BRUCON 2011
- Dr L. Ball - Presentation at the Dundee Café Science initiative. The subject was Emotional Computing. 28th March, 2011.
- Dr Ferguson presented a talk entitled "Cybercrime: Threat or Promise?" as part of the SICSA Christmas Lecture 2012
- Dr R.I. Ferguson - Presentation at the Dundee Café Science initiative. - Oct 2012 - Digital Forensics vs Sex, Drugs and Rock and Roll
- Dr N. Coull – Holyrood Conference on Cybersecurity (Feb. 2013)
- Members of the SRG are frequently speakers at schools in the Tayside and Fife area on issues related to cybersecurity