Security Research Group

cybersecurity.abertay.ac.uk

Personnel and expertise

Prof. Karen Renaud	- *usable security*
Dr Ian Ferguson (SRG coordinator)	- *digital forensics*
Dr Natalie Coull	- *ethical hacking*
Dr Jackie Archibald	- *usable security*
Mr Colin McLean	- *ethical hacking*
Dr Andrea Szymkowiak	- *emotional biometrics*
Mr David McLuskie	- *network security and ethical hacking*
Dr Adam Sampson	- *security in software engineering*
Dr. Xavier Bellekens	- *security and privacy in the Internet of Things*
Dr Lynsay Shepherd	- *usable security*
Dr Gavin Hales	- *digital forensic visualisation*
Mr Scott Mitchell	- *PhD student: Countermeasures to digital piracy*
Dr Ethan Bayne	- *Digital Forensics Rapid Analysis*
Mr James Sutherland	*-PhD student: Hardware security*
Ms Tayyaba Nafees	- *PhD student: Empiric origins of security flaws*
Mr Jason Johnstone	*-PhD student: A sociological study of the ethical hacking community.*

All the above can be contacted via email by using <first initial>.<lastname>@abertay.ac.uk +44 (0)1382 308 601

Interests

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

Ethical Hacking – developing techniques, methodologies and tools to assist in security assessment and penetration testing of corporate, personal, mobile and cloud platforms.

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 – emotional biometrics – recognising users and their emotional state, 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.

Serious Games for Cybersecurity training and education

Intelligence Systems – Open Source Intelligence and counterterrorism.

Smartgrid Security – the Internet of Things and critical infrastructure protection.

Recent Successes

- An Innovation Voucher award (Wih Droman Ltd) looking at the use of serious games to support the training of police officers in cybercrime response.
- An ongoing cooperation with the Scotish Business Resilience Centre providing cybersecurity assessment to SMEs using ASSAM (Abertay SME Security Assessment Methodology)
- 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.
- SIPR funded project on the development of secure hardware for managing offenders in the community
- SIPR funded project for the development of mobile apps to support child-interviewing by law-enforcement.
- 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 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 R.I. Ferguson

Id Inquiries Ltd – Development of a novel Digital Forensic technique for investigation of DRM abuse.

A KTP funded project (£120K) which looked at the application of ethical hacking techniques in a Digital Forensic context to facilitate the acquisition of evidence of Digital Rights Management abuses.

Dr R.I.Ferguson/Dr N.Coull

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

biometrics

Biometrics is about the identification of people, most often used for controlling access to secure spaces. In order to do that, we can either use physiological traits, such as finger prints, retinal and face image, or behavioural traits, such as typing on a keyboard or observing someone's gait, for example. In addition, the identification of emotional states has become more relevant in recent years and we describe this as emotional biometrics.

Dr Andrea Szymkowiak

Wireless Network Sensors for Safety-Critical Infrastructures.

This project lead to the assessment of wireless sensors for nuclear power plants and high risk environments. A number of factors were analysed such as security and privacy by design. Numerous attacks were investigated and a threat assessment methodology was provided. This project also lead to the design and implementation of two different Intrusion Detection Systems, and Honeypots making use of Big Data and Deep Neural Networks and Graphics Processing Units (GPUs).

Mr X. Bellekens

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

[1] www.sicsa.ac.uk

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

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.

Mr Ethan Bayne

Dissemination

Some Recent Publications

Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures, X. J. A. Bellekens, A. Seeam, K. Nieradzinska, C. Tachtatzis, A. Cleary, R. Atkinson, I. Andonovic, Wireless World Research Forum Meeting 35 (WWRF35), Copenhagen, Danemark, 2015

GLoP: Enabling Massively Parallel Incident Response Through GPU Log Processing, X. J. A. Bellekens, C. Tachtatzis, R. C. Atkinson, C. Renfrew, T. Kirkham, 7th International Conference of Security of Information and Networks, SIN 2014, Glasgow, UK, September, 2014.

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.

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.A., Archibald, J. and Ferguson, R.I. 2013. *Perception of risky security behaviour by users: survey of current approaches*. In: L. Marinos, I. Askoxylakis, eds. Human Aspects of Information Security, Privacy, and Trust. Berlin: Springer. 2013, pp.176-185 [online].

Available from DOI: http://dx.doi.org/10.1007/978-3-642-39345-7_19

Shepherd, L.A., Archibald, J. and Ferguson, R.I. 2014. *Reducing risky security behaviours: utilising affective feedback to educate users*. Future Internet. 6(4): pp.760-772. Available from DOI: http://dx.doi.org/10.3390/fi6040760

Ahmad, N., Szymkowiak, A. and Campbell, P.A., 2013. *Keystroke dynamics in the pre-touchscreen era.* Frontiers in Human Neuroscience 7. http://dx.doi.org/10.3389/fnhum.2013.00835

Walker, N., Coull, N, Ferguson, R.I. And Milne, A. *A Method for Resolving Security Vulnerabilities Through the Use of Design Patterns*, in Cyberpatterns (Eds Blackwell, C. and Hong, Z), Springer, 978-3-319-04446-0, p.149-155 (2014)

Russell, D., Bradley, D.A., McLeod, A. White, R., Ferguson, R.I., and Isaacs, J., "*The Internet of Things – The Future or the End of Mechatronics*", in Mechatronics D-14-00540R1 (Feb 2015)

Bayne, E. Ferguson, R.I. And Isaacs, J. *OpenCL Accleration of Digital Forensic Methods* in Proc. Of Intl. Conf. On Cybercrime, Security and Digital Forensics (CyFor2014), University of Strathclyde, Glasgow (2014)

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.

- Demonstration of Ethical Hacking techniques at the Scottish Government National Cyber-security Strategy launch event.
- 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
- Colin Maclean - Ethical Hacking presentation at BRUCON 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