2014


Security Research Institute, Edith Cowan University
The Proceedings of

12th Australian Digital Forensics Conference

1-3 December, 2014

ECU Joondalup Campus, Perth, Western Australia
Conference Foreword

This is the third year that the Australian Digital Forensics Conference has been held under the banner of the Security Research Institute, which is in part due to the success of the security conference program at ECU. As with previous years, the conference continues to see a large number of papers with a number of high quality submissions from local and international authors. All submissions were subject to a double blind peer review process and we had an acceptance rate of approximately 80%.

Conferences such as these are simply not possible without willing volunteers who follow through with the commitment they have initially made, and I would like to take this opportunity to thank the conference committee for their tireless efforts in this regard. These efforts have included but not been limited to the reviewing and editing of the conference papers, and helping with the planning, organisation and execution of the conference. Particular thanks go to those international reviewers who took the time to review papers for the conference, irrespective of the fact that they are unable to attend this year.

To our sponsors and supporters also a vote of thanks for both the financial and moral support provided to the conference. Finally, to the student volunteers and staff of the ECU Security Research Institute – your efforts as always are appreciated and invaluable.

Yours sincerely

Conference Chair
Professor Craig Valli, Director, Security Research Institute

Congress Organising Committee
Congress Chair: Professor Craig Valli
Committee Members:  Dr David Brooks
          Mr Clinton Carpene
          Mr Jeff Corkill
          Mr Michael Coole
          Mr David Cook
          Mr Michael Crowley
          Mr Peter Hannay
          Dr Mike Johnstone
          Mr Patryk Szewczyk
          Mr Krishnun Sansurooah
          Dr Zubair Baig
          Associate Professor Andrew Woodward
          Associate Professor Trish Williams
          Professor Bill Hutchinson
          Professor Nara Srinivasan
Congress Coordinator:  Ms Emma Burke
# Table of Contents

TOWARDS A SET OF METRICS TO GUIDE THE GENERATION OF FAKE COMPUTER FILE SYSTEMS................................................................................................................................. 5  
*Ben Whitham*

LOCATIONAL WIRELESS AND SOCIAL MEDIA-BASED SURVEILLANCE......................................................... 17  
*Maxim Chernyshev*

THE ZOMBIES STRIKE BACK: TOWARDS CLIENT-SIDE BEEF DETECTION.................................................. 26  
*Maxim Chernyshev, Peter Hannay*

FORENSIC EXAMINATION AND ANALYSIS OF THE PREFETCH FILES ON THE BANKING TROJAN MALWARE INCIDENTS................................................................................................................................. 35  
*Andri P Heriyanto*

LISTENING TO BOTNET COMMUNICATION CHANNELS TO PROTECT INFORMATION SYSTEMS.................................................. 44  
*Brian Cusack, Sultan Almutairi*

UP-DATING INVESTIGATION MODELS FOR SMART PHONE PROCEDURES........................................... 53  
*Brian Cusack, Raymond Lutui*

SUITABILITY OF LACUNARITY MEASURE FOR BLIND STEGANALYSIS.......................................................... 64  
*Ahmed Ibrahim*

A FORENSICALLY-ENABLED IAAS CLOUD COMPUTING ARCHITECTURE................................................................................. 75  
*Saad Alqahtany, Nathan Clarke, Steven Furnell, Christoph Reich*

A USER-ORIENTED NETWORK FORENSIC ANALYSER: THE DESIGN OF A HIGH-LEVEL PROTOCOL ANALYSER............................................................................................................................................................................. 84  
*D. Joy, F. Li, N.L. Clarke, S.M. Furnell*

THE IMPACT OF CUSTOM ROM BACKUPS ON ANDROID EXTERNAL STORAGE ERASURE......................... 94  
*Haydon Hope, Peter Hannay*

A FORENSIC OVERVIEW OF THE LG SMART TV................................................................................................. 102  
*Iain Sutherland, Konstantinos Xynos, Huw Read, Andy Jones, Tom Drange*

RAPID FORENSIC CRIME SCENE ANALYSIS USING INEXPENSIVE SENSORS................................................ 109  
*Dan Blackman*

FINDING EVIDENCE OF WORDLISTS BEING DEPLOYED AGAINST SSH HONEYPOTS - IMPLICATIONS AND IMPACTS.................................................................................................................................................................................. 114  
*Priya Rabadia, Craig Valli*