

# The Proceedings of 2018 Cyber Forensic & Security International Conference



“Better Protection for Stronger Communities”



**The Proceedings of**

**2018**

**Cyber Forensic & Security**

**International**

**Conference**

**Edited by**

**Brian Cusack & Raymond Lutui**



# Foreword

We are delighted to welcome you to the 2018 Cyber Forensic and Security International Conference in the Kingdom of Tonga. These conferences have been running since 2004 to bring like-minded people together to evaluate Governance, Risk, and Compliance (GRC) issues of the day, and to solidify International networking for improved public and professional practice. We have accepted 28 peer reviewed papers from 22 different nations and present four keynote addresses from esteemed International speakers. The theme of the conference is “Better Protection for Stronger Communities”, which has been chosen to reflect the impact and social value of effective security systems. The Pacific – as with everywhere – is open to cyber-attack and the negative social and economic disadvantages it brings. It is time a stronger effort is made to educate and train effective defences for safer, stronger and more resilient communities.

The conference would not have been possible without the sponsorship of Christ’s University in Pacific. Also the many business sponsors, and the tireless work of the Research Institute Manager, Siaso (George) Maeakafa, to make the event possible. The Rev Dr Liufau Saulala, the Vice Chancellor of Christ’s University in Pacific permitted the hosting and has marshalled an army of University support personnel and members of the Tokaikolo Christian Church to facilitate the conference services and warm welcome. He is acknowledged in appreciation and the Conference Organising Committee communicate their gratitude. The peer reviewers of the conference papers are also thanked for their reviews and wise advice. There are many other people, such as Bryce Coad, who has provided generous technical support and assistance with the publication, whom have all made this event successful.

The Conference Proceeding is structured to communicate the published content of the event. The first section presents the keynote addresses, and the second the short papers. Each paper has received two independent reviews by experts and the authors asked to respond to the comments. In the second section the long papers are presented in three sub-sections representing the three topic streams: Assurance, Forensics, and Security. In the first section the keynote presentations address the conference theme of “Better Protection for Stronger Communities”, by reviewing Tonga’s digital security preparation, maritime digital safety, E-Government security, and how to discover evidence in common Windows environments. These four divergent addresses make a strong statement regarding the scope of community preparedness for digital resilience.

In the second section five topical papers are presented on E-Government, the latest techniques in evidence recovery, Pacific cybersecurity co-operation, malware detection and a tradition digital security defence. Each of these topics are relevant and helpful in understanding

current challenges, and what is useful from past perspectives. The third section is more diverse and divided into three themes. The Assurance theme captures provisions made to provide confidence in the digital services and their contexts. The first paper concerns fraud detection, the second security controls for E-Government, the fourth E-Government implementation, and the fifth Cloud services evaluation and assurance. The third paper is interesting. It addresses the cost problem of implementing controls and provides an automated solution. The sixth paper is also edge cutting: blockchain application to health services in Papua New Guinea.

The last two sub-sections of the long papers take the topics of forensics and security and elaborate different perspectives on the theme “Better Protection for Stronger Communities”. The forensic papers concern investigation techniques, tools, big data, traceback; and, interestingly the role of the digital forensic Lab manager. The final paper of the sub-section raises a challenging problem – evidence collection in Augmented Reality (AR) and the potential legal liabilities. The final sub-section addresses security from the perspectives of Law Enforcement, critical infrastructures, and a raft of contexts that include: IoT, Wireless, Cloud, WBNs, Medical, and Tongan organisations.

The full schedule of events is available in the timetable published online and in the conference folder. This includes rooms, maps and scheduled times for presentations, events and transport. Many of these things will be updated on a daily basis to assure the smooth running of the program.

Enjoy your time with us, and be free to ask for help!

Prof Brian Cusack

Chair Organising Committee

[brian.cusack@aut.ac.nz](mailto:brian.cusack@aut.ac.nz)

# Contents

## Keynote Addresses

1. .... Page 11  
Tonga's Cyber Security Preparation and Its Economic Advantages  
*Hon. Siaso Sovaleni, Kingdom of Tonga*
2. .... Page 12  
Security Strategy for E-Government  
*Dr Stephen Thorpe, New Zealand*
3. .... Page 13  
Cyber Maritime Security and Safety  
*Prof Andy Jones, United Kingdom*
4. .... Page 14  
Recovering Windows Artefacts  
*Jung Son, Korea*

## Short Papers

1. .... Page 17  
The Importance of Information Security Research for the National Economy  
*Stephen Thorpe, AUT University*
2. .... Page 21  
The Recovery of Windows Artefacts  
*Jung Son, CFO, Auckland*
3. .... Page 27  
Review of the CROP ICT Working Group and Pacific Cybersecurity  
Development  
*Ian Thompson, University South Pacific, Fiji*
4. .... Page 30  
Towards a Method for Detecting Botnet Code on IoT Devices  
*Ashley Woodiss-Field and Michael N Johnstone, Security Research Institute,  
WA, Australia*

5.	.....	Page 35
	The Evaluation of Security Risk Assessment Models <i>Sid Sirisukha, Stamford University, Bangkok, Thailand</i>	

## **Long Papers**

### **(Assurance Stream)**

1.	.....	Page 39
	Management Fraud: Prevention, Detection and Response <i>Tauaho Ahokovi, Christ's University in Pacific</i>	
2.	.....	Page 47
	Establishing Security Controls in E-Government Planning <i>Gerard Ward, AUT University</i>	
3.	.....	Page 57
	A Methodology for Selecting Security Controls to Assure Business System Value Realization <i>Maher Al-Khazraji, UNITEC University</i>	
4.	.....	Page 69
	Securely Implementing E-Government Vision and Strategy in a Developing Country <i>Paula R Lutui, George Maeakafa, Christ's University in Pacific</i>	
5.	.....	Page 79
	A Synthesis Technique for Cloud Life-Cycle Evaluation and Quality Assurance <i>Eghbal Ghazizadeh, AUT University</i>	
6.	.....	Page 87
	Protecting the Rights of the Producer of the IoT Data and Assuring Privacy of Ownership <i>Reza Khaleghparast, Nelson Polytechnic University</i>	

### **(Digital Forensic Stream)**

1.	.....	Page 99
	A Model to Facilitate Collaborative Digital Forensic Investigations for Law Enforcement: The Royal Oman Police as a Case Study <i>Younis Al Husaini, Haider Al-Khateeb*, Matthew Warren, Lei Pan, Deakin University and University of Wolverhampton*</i>	

2.	.....	Page 109
	Evaluating Network Tools Error Rates for Compliance Reporting <i>Bryce Antony, AUT University</i>	
3.	.....	Page 117
	Comparing Mobile Phone Forensic Tool Performances <i>Stephanie Brennadiva, AUT University</i>	
4.	.....	Page 127
	Improving Image Retrieval Techniques for Big Forensic Data Sets <i>Dan Fraser, QSG, Australia</i>	
5.	.....	Page 135
	The Role of Digital Forensic Laboratory Manager <i>Tupou Bryce, Christ's University in Pacific</i>	
6.	.....	Page 145
	Hop Count ICMP Traceback Method Simulation & Evaluation <i>Zhuang Tian, AUT University</i>	
7.	.....	Page 155
	The Impact of Augmented Reality on Digital Evidence Collection <i>Kaushik Sundararajan, AUT University</i>	

**(Security Stream)**

1.	.....	Page 165
	Security Visualization Intelligence Model for Law Enforcement Investigations <i>Jeffery Garae, Ryan K. L. Ko, Mark Apperley, Silvino J. Schlickmann*, The University of Waikato and Interpol*</i>	
2.	.....	Page 179
	Penetration Plan for Critical Infrastructure Protection <i>Amr Mahmoud, AUT University</i>	
3.	.....	Page 187
	Cyber Security Vulnerabilities in Tonga <i>Siuta Lau Laupea'alu, Te Taka Keegan, University of Waikato</i>	
4.	.....	Page 195
	Authentication and Access Control for Health Information Exchange in PNG using Blockchain Technology <i>Alan T Litchfield, Dean Foy, and Raymond Lutui, Daltron PNG Ltd</i>	
5.	.....	Page 207

	An Analysis of Wireless Security Vulnerabilities in Nuku'alofa: Wardriving Study <i>Osai Tete'imoana and Raymond Lutui, Christ University in Pacific</i>	
6.	.....	Page 217
	Developing Secure Networks for IoT Communications <i>Bryce Antony, AUT University</i>	
7.	.....	Page 229
	Cloud Security Issues that Impact Privacy in Digital Identity Management <i>Eghbal Ghazizadeh, AUT University</i>	
8.	.....	Page 243
	Securing Privacy Vulnerabilities in Wireless Body Networks <i>Adekemi Adedokun, University of Technology Malaysia</i>	
9.	.....	Page 255
	<b>Data Security Assessment for Organisations in Tonga</b> <b><i>Siuta Laulaupea'alu, Te Taka Keegan, University of Waikato</i></b>	
10.	.....	Page 265
	Treating Wireless Medical System Risks for Usability and Safety <i>Akar Kyaw, Whitireia University</i>	