13th Australian Digital Forensics Conference

THE NEED OF MALWARE PROFILING FOR ANDROID SMARTPHONE FORENSICS

The prevalence of Android smartphones and the immense growth of Android malware create significant numbers of malware incidents that require forensics handling. Certain smartphone forensic tool has incorporated anti-virus databases in their device for malware detection process. However, examiners should be aware that most of anti-virus application uses known patterns or signatures for malware detection that might not be effective for unknown malware. Moreover, many advanced malware are known using specific techniques to hide its presence from anti-virus detection and for anti-forensics technique. Beside the malware detection requirement, the examiner needs to do the Malware Profiling for obtaining the information such as a purpose of malware and how to achieve it and any other information. Many tools and techniques for Android malware analysis can be used for Malware Profiling process. However, this procedure should consider the forensically sound process. The research shows several tools and techniques for supporting the process and proposes the workflow for Malware Profiling. The research uses Zeus-in-the-Mobile (ZitMO) as the malware sample for showing how examiner can perform the Malware Profiling based on the proposed workflow.

MAPPING THE LAWS WHICH APPLY TO INTERCEPTING WIRELESS COMMUNICATIONS IN A WESTERN AUSTRALIAN LEGAL CONTEXT

The rapid evolution and deployment of WiFi technology creates a new environment where offenders can intercept and obtain sensitive information for use in the commissioning of further criminal activity. This paper explores how the law applies to and protects the wireless communications environment, with specific focus on the interception of WiFi data communications.

THE CHALLENGE OF SEIZING AND SEARCHING THE CONTENTS OF WI-FI DEVICES FOR THE MODERN INVESTIGATOR

To the modern law enforcement investigator, the potential for an offender to have a mobile device on his or her person, which then connects to a WiFi device, may afford evidence to place them at a scene, at a particular time. However whilst tools to interrogate the mobile device and WiFi networks it has connected to, have undergone significant development, little research has been conducted with regards to interrogating WiFi routers and the evidence they may contain.

STEGANOGRAPHIC THREATS - FAIRYTALE OR FACT?

Almost since the birth of the Internet, there has been a fear that steganographically encoded threats would be used to bring harm. Serious consideration has been given to the idea that merely downloading an image could introduce malware. And yet, for decades, evidence of this type of channel has been missing in action. There is still an unwritten assumption that images are harmless. Many vendors have implicitly avoided producing defences against steganographic threats. Is it truly impossible to make a widely harmful exploit this way or have malicious actors accepted general wisdom? Recent developments suggest that there may be a new chapter ahead of us in this area. So, are we seeing a new frontier in exploit development or is there another false dawn for steganographic threats?
TOWARDS A STANDARDISED STRATEGY TO COLLECT AND DISTRIBUTE APPLICATION SOFTWARE ARTIFACTS

Reference sets contain known content that are used to identify relevant content or filter irrelevant content. Application profiles are a type of reference set that contain digital artifacts associated with application software. An application profile can be compared against a target data set to identify relevant evidence of application usage in a variety of investigation scenarios. This research works towards a standardised strategy to collect and distribute application software artifacts using application profiles. An advanced technique for creating application profiles was designed using a formalised differential analysis strategy. The design was implemented in a live differential forensic analysis tool, LiveDiff, to automate and simplify data collection. A storage mechanism was designed based on a previously standardised forensic data abstraction. The design was implemented in a new data abstraction, Application Profile XML, to provide storage, distribution and automated processing of collected artifacts.

IMPROVING THE DETECTION AND VALIDATION OF INLAND REVENUE NUMBERS

Forensic analysis commonly involves searching an investigation target for personal identifiable information. An Inland Revenue Department (IRD) number is used for taxation purposes in New Zealand and can provide evidence of perpetrator identity, transaction information or electronic fraud. This research has designed and implemented a bulk_extractor feature scanner to detect and validate IRD numbers (features). The IRD scanner has been tested on a known data set to ensure tool functionality. A large real world data set was then used to determine scanner effectiveness in a realistic investigation scenario. Real world data set testing highlighted a high number of unrelated features detected by the scanner. To combat this, a novel post processing technique was implemented to identify forensically interesting IRD numbers by performing feature context searching. The post processing findings proved that feature context searching is an effective data reduction technique that identified a low number of directly relevant IRD numbers.

THE APPLICATION OF DATA MINING TO INTRUSION DETECTION APPROACHES

Cyber-security has become more prevalent as more organisations are relying on cyber-enabled infrastructures to conduct their daily activities. Subsequently cybercrime and cyber-attacks are increasing. An Intrusion Detection System (IDS) is a cyber-security tool that can be used to mitigate against cyber-attacks. An IDS is a system deployed to monitor network traffic and trigger an alert when unauthorised activity is detected. It is important for IDSs to accurately identify cyber-attacks against assets on cyber-enabled infrastructures, while also being efficient at processing current and predicted network traffic flows. The purpose of the paper is to outline the importance of developing an accurate and effective intrusion detection approach that can be deployed by an IDS. Further research aims to develop a hybrid data mining intrusion detection approach that uses Decision Tree classifications and Association Rules to extract rules using the classified data.

AN OVERVIEW OF BLUETOOTH DEVICE DISCOVERY AND FINGERPRINTING TECHNIQUES - ASSESSING THE LOCAL CONTEXT

The ubiquitous nature of portable communication devices presents a number of opportunities for automated device discovery, tracking and possible owner identification. Consumer devices such as smartphones, tablets, wearables, laptops and vehicle
entertainment systems commonly support the 802.15.1 (Bluetooth) wireless communication protocol that enables a variety device discovery and fingerprinting techniques. We provide an overview of these techniques encompassing those native to the protocol as well as those that are possibly protocol-agnostic due to their inherently generic nature. We then introduce a comparison study that sets out to examine and quantify the effectiveness of selected techniques in the field. To assess the potential viability of this study, we perform local context evaluation based on location-aware inquiry scanning and discuss the results of the exploratory data collection.

SECURITY ASSESSMENT OF IOT DEVICES: THE CASE OF TWO SMART TVs

Being increasingly complex devices, smart TVs are becoming more capable and have the potential to receive, store, process and transmit considerable amounts of personal data. These capabilities also represent several diverse attack surfaces potentially rendering these devices highly vulnerable. The emergence and high adoption rate of smart TVs have been drawing notable interest from security researchers and industry. We utilise an attack surface area-based approach to assess the security of two modern smart TVs from different vendors and describe some of the possible multi-surface attacks that can be carried out against these devices.

THE SPY IN YOUR POCKET: SMARTPHONES AND GEO-LOCATION DATA

The integration of Global Positioning Systems and Smartphones has seen the significance of location based services rise. Geo-location data could prove to be an invaluable source of evidence in a forensic investigation. An attempt to extract geo-location data from an iPhone4s and Huawei Ascend G526 in a forensically sound manner revealed significant geo-location data embedded within geo-tags within photos taken on the devices. Other limited evidence was located on the devices.

CYBER BLACK BOX: NETWORK INTRUSION FORENSICS SYSTEM FOR COLLECTING AND PRESERVING EVIDENCE OF ATTACK

Forensics and investigation are always executed after the attack, once the system is compromised and often results in the loss of useful instant evidence. Since there is no log information necessary for analyzing an attack cause after the cyber incident occurs, it is difficult to analyze the cause of an intrusion even after an intrusion event is recognized. Moreover, in an advanced cyber incident such as advanced persistent threats, several months or more are expended in only analyzing a cause, and it is difficult to find the cause with conventional security equipment. In this paper, we introduce a network intrusion forensics system for collecting and preserving the evidence of an intrusion, is called Cyber Black Box, which is deployed in local area network environment. It quickly analyzes a cause of an intrusion event when the intrusion event occurs, and provides the function of collecting the evidence data of the intrusion event. It also describes the experimental results of the network throughout performance by deploying our proposed system in an experimental testbed environment.

IMAGE SIMILARITY USING DYNAMIC TIME WARping OF FRACtAL FEATURES

Hashing algorithms such as MD/SHA variants have been used for years by forensic investigators to look for known artefacts of interest such as malicious files. However, such hashing algorithms are not effective when their hashes change with the slightest alteration in the file. Fuzzy hashing overcame this limitation
to a certain extent by providing a close enough measure for slight modifications. As such, image forensics is an essential part of any digital crime investigation, especially in cases involving child pornography. Unfortunately such hashing algorithms can be thwarted easily by operations as simple as saving the original file in a different image format. This paper introduces a novel technique for measuring image similarity using Dynamic Time Warping (DTW) of fractal features taken from the frequency domain. DTW has traditionally been used successfully for speech recognition. Our experiments have shown that it is also effective for measuring image similarity while tolerating minor modifications, which is currently not capable by state-of-the-art tools.

MOBILE DEVICE DAMAGE AND THE CHALLENGES TO THE MODERN INVESTIGATOR

Mobile Forensics has developed into an area of significant concern to law enforcement agencies and their counterparts, specifically as a result of individuals moving away from using traditional computers and focusing attention to their mobile device. Due to the smart phone being almost permanently attached to the person or in near proximity, can be a significant source of investigators and can mean the difference between proving guilt or innocence. Tools have been long been established, which provide agencies the ability and encapsulated expertise to download and easily produce reports for the mobile device and how it had been used. However whilst these tools work for the majority of devices in near perfect working condition they fail in cases where the phone is even slightly damaged. Many of the tools also require the investigator to unlock the phone or enable a feature before it can be downloaded. Should part of the phone be malfunctioning or if it prevents a feature or unlock from occurring, the ability to obtain the evidence will be reduced. Whilst the devices are surprisingly resilient at times, damage by throwing the device into a fire or snapping the logic board in half, will ultimately cause the device to be inoperable and beyond repairable. In these cases, how can the investigator even identify the model of device, considering parts of the device, including identification stickers, may have melted off or be missing? In these scenarios repairing the phone via changing the majority of the hardware from ‘donor’ phone cannot be conducted, as they are beyond repairable. There is also no chance of being able to re-join the parts of a double or triple layer logic board and a re-joining a single layer logic board is both time and labour intensive. Even then there is no guarantee the phone will work again. To counter these issues, significant monetary value needs to be invested in equipment and training to skill forensic investigators with the skills and ability in Chip-Off forensics and Ball Grid Array (BGA) rework. This skill means the small chips from the logic board can be removed without causing damaged to their delicate legs or body and the data they contain interpreted. Once interpreted, the investigator then has the ability to find what evidence was located on the device and hopefully leading to a conviction of guilt.

FILE SYSTEM MODELLING FOR DIGITAL TRIAGE: AN INDUCTIVE PROFILING APPROACH

Digital Forensic Triage is the initial, rapid screening of electronic devices as a precursor to full forensic analysis. Triage has numerous benefits including resource prioritisation, greater involvement of criminal investigators and the rapid provision of initial outcomes. In traditional scientific forensics and criminology, certain behavioural attributes and character traits can be identified and used to construct a case profile to focus an investigation and narrow down a list of suspects. This research leverages the habitual nature of human behaviour and applies it to the digital medium,
developing a tool to profile how offenders utilise and structure file systems on their digital devices. The need for this research will be outlined by drawing on existing digital triage methods from literature with its utility highlighted through the use of four test cases. Finally, future research direction from this work will be identified.

A CYBER BLACKBOX FOR COLLECTING NETWORK EVIDENCE

In recent years, the hottest topics in the security field are related to the advanced and persistent attacks. As an approach to solve this problem, we propose a cyber blackbox which collects and preserves network traffic on a virtual volume based WORM device, called EvidenceLock to ensure data integrity for security and forensic analysis. As a strategy to retain traffic for long enough periods, we introduce a deduplication method. Also this paper includes a study on the network evidence which is collected and preserved for analyzing the cause of cyber incident. Then, a method is proposed to suggest a starting point for incident analysis to a forensic practitioner who has to investigate on the vast amount of network traffic collected using the cyber blackbox. Experimental results show this approach is effectively able to reduce the amount of data to search by dividing doubtful flows from normal traffic. Finally, we discuss the results from a forensically meaningful point of view and present further works.

COMPARISON OF LIVE RESPONSE, LINUX MEMORY EXTRACTOR (LiME) AND MEM TOOL FOR ACQUIRING ANDROID’S VOLATILE MEMORY IN THE MALWARE INCIDENT

There is an increasing interest in Android volatile memory acquisition and analysis since advanced malware might leave their footprints only in the RAM. However, current smartphone forensics guidance has not stated an acquisition of memory based on its volatility order as many as well-known computer forensic guidances have proposed. Hence, there is a conundrum between the needs and the availability of tools and workflow for acquiring the volatile memory on the Android’s smartphone. The research compares three different tools for acquiring the volatile memory: Live Response, Linux Memory Extractor (LiME) and Mem tool and reveals the analysis’ output from related approaches. The research uses Backdoor.AndroidOS.Obad as a malware sample which known as one of the most sophisticated mobile Trojan. The research shows that LiME and Volatility Framework have gathered the most robust findings. However, LiME is considered not feasible and had significant constraints that might deter its usage. On the other hand, live response is proof that significant findings can be obtained. However, the approach should be taken carefully to minimize the impact on unallocated data in the RAM.

MINING SOCIAL NETWORKING SITES FOR DIGITAL EVIDENCE

OnLine Social Networking sites (SNS) hold a vast amount of information that individuals and organisations post about themselves. Investigations include SNS as sources of evidence and the challenge is to have effective tools to extract the evidence. In this exploratory research we apply the latest version of a proprietary tool to identify potential evidence from five SNS using three different browsers. We found that each IT artefact influenced the scope of the evidence extracted. In previous research it has been shown that different open source and proprietary tools influence the scope of evidence obtained. In this research it was asked, what variation in the scope of evidence extraction can be expected between different browsers? The implications of this exploratory research is for precaution. The
choice of a browser to investigate a SNS directly influences the scope of digital evidence obtained.

13th Australian Information Security Management Conference

EVALUATING SINGLE SIGN ON SECURITY FAILURE IN CLOUD SERVICES

The business use of cloud computing services is motivated by the ease of use and the potential financial cost reductions. Service failure may occur when the service provider does not protect information or when the use of the services becomes overly complex and difficult. The benefits also bring optimisation challenges for the information owners who must assess the service security risk and the degree to which new human behaviours are required. In this research we look at the risk of identity theft when ease of service access is provided through a Single Sign On (SSO) authorisation and ask: What are the optimal behavioural expectations for a Cloud service information owner? Federated identity management is a well-developed design literature for solutions to optimising human behaviours in relation to the new technologies. We briefly review the literature and then propose a working solution that optimises the trade-off between disclosure risk, human user risk and service security. Both breech and non-use of a system are failures.

A SURVEY AND METHOD FOR ANALYSING SOHO ROUTER FIRMWARE CURRENCY

Network routers are a core component of contemporary SoHo networks. The firmware within these devices provides routing, control and monitoring functionality coupled with mechanisms to ensure a secure and reliable network. End-users are typically reliant on manufacturers to update and provide timely firmware releases to mitigate known vulnerabilities. An investigation was undertaken to identify the underlying software components used in the firmware of currently available SoHo network devices. Firmware from 37 devices was deconstructed to identify potential security issues; in each instance, the firmware images were found to include vulnerabilities, obsolete software and out-of-date operating system components. 95% of the deconstructed firmware was based on Linux. The Linux kernels identified were discontinued and are no longer actively maintained. This paper demonstrates a method for undertaking the analysis and summaries the outcomes of the research.

TOWARDS DYNAMIC ADAPTION OF USER’S ORGANISATIONAL INFORMATION SECURITY BEHAVIOUR

The weakest link in the field of information security that has been identified in the literature is the organisation’s employees. Information security policy compliance is one of the main challenges facing organisations today. Although implementing technical and procedural measures clearly helps to improve an organisation’s information security, the human factor or the employees’ compliance with these measures is the key to success. However, organisations are now having some issues regarding the extent of employee adherence to policy. The problem of employees being unaware or ignorant of their responsibilities in relation to information security is still an open issue. The proposed idea in this paper will seek to enhance end user adherence to information security policies by proposing a framework for security policy compliance monitoring and targeted awareness raising. The foremost aim of this framework is to increase users’ awareness of the importance of following information security policies. Continuously subjecting users to targeted awareness and monitoring their adherence to information security policies should enhance the effectiveness of such awareness efforts. The
proposed framework is a part of on-going research and is intended to provide a foundation for future research on a dynamic adaption of users’ behaviour with information security policies.

**URDU TEXT STEGANOGRAPHY: UTILIZING ISOLATED LETTERS**

This paper proposed an imperceptible and high payload feature based approach, which hides a secret message into Urdu text cover media by utilizing all isolated letters. Existing techniques are less imperceptible and not robust against text steganalysis while some of the text steganography schemes are failed to provide the better hidden capacity rates. Previous lexical based and syntax based schemes are ineffective to provide the better hidden volume, and image based approaches are not robust against format attacks. Feature based approaches are more perceptible and cannot resist against visual attacks. This article presents an improved algorithm that encompasses all isolated letters of Urdu text for data hiding to provide better hidden capacity. Furthermore, the presented technique is more secured by using strong public key encryption algorithm. In addition, the scheme is also imperceptible, since it does not affect the external appearance of the text. Implementation results show that the proposed text steganography technique provides high hidden payload.

**RANSOMWARE: EMERGENCE OF THE CYBER-EXTORTION MENACE**

Ransomware is increasingly posing a threat to the security of information resources. Millions of dollars of monetary loss have been afflicted on end-users and corporations alike through unlawful deployment of ransomware. Through malware injection into end-user devices and subsequent extortion of their system or data, ransomware has emerged as a threat requiring immediate attention and containment by the cyber-security community. We conduct a detailed analysis of the steps of execution involved in ransomware deployment to facilitate readiness of the cyber-security community in containing the rapid proliferation of ransomware. This paper examines the evolution of malware over a period of 26 years and the emergence of ransomware in the cyber-threat landscape. Key findings on the evolution of ransomware and its use of emerging technologies are presented.

**TIMING ATTACK DETECTION ON BACNET VIA A MACHINE LEARNING APPROACH**

Building Automation Systems (BAS), alternatively known as Building Management Systems (BMS), which centralise the management of building services, are often connected to corporate networks and are routinely accessed remotely for operational management and emergency purposes. The protocols used in BAS, in particular BACnet, were not designed with security as a primary requirement, thus the majority of systems operate with sub-standard or non-existent security implementations. As intrusion is thus likely easy to achieve, intrusion detection systems should be put in place to ensure they can be detected and mitigated. Existing intrusion detection systems typically deal only with known threats (signature-based approaches) or suffer from a high false positive rate (anomaly-based approaches). In this paper we present an overview of the problem space with respect to BAS, and suggest that state aware machine learning techniques could be used to discover threats that comprise a collection of legitimate commands. We provide a first step showing that the concept can be used to detect an attack where legitimate write commands being sent in rapid succession may cause system failure. We capture the state as a ‘time since last write’ event and use a basic
artificial neural network classifier to detect attacks.

**SELECTION OF PENETRATION TESTING METHODOLOGIES: A COMPARISON AND EVALUATION**

Cyber security is fast becoming a strategic priority across both governments and private organisations. With technology abundantly available, and the unbridled growth in the size and complexity of information systems, cyber criminals have a multitude of targets. Therefore, cyber security assessments are becoming common practice as concerns about information security grow. Penetration testing is one mitigation strategy used to mitigate the risk of cyber-attack. Penetration testers attempt to compromise systems potentially using the same tools and techniques as malicious attackers thus attempting to identify vulnerabilities before an attack occurs. This research details a gap analysis of the theoretical vs. the practical classification of nine penetration testing frameworks and/or methodologies. Additionally, an analysis of two of the frameworks was undertaken to evaluate each against six quality characteristics. The characteristics were fitted into a modified version of an ISO quality model.

**BEHAVIOR-BASED ANOMALY DETECTION ON BIG DATA**

Recently, cyber-targeted attacks such as APT (Advanced Persistent Threat) are rapidly growing as a social and national threat. It is an intelligent cyber-attack that infiltrates the target organization and enterprise clandestinely using various methods and causes considerable damage by making a final attack after long-term and through preparations. These attacks are threatening cyber worlds such as Internet by infecting and attacking the devices on this environment with the malicious code, and by destroying them or gaining their authorities. Detecting these attacks requires collecting and analysing data from various sources (net-work, host, security equipment, and devices) over the long haul. Therefore, we propose the method that can recognize the cyber-targeted attack and detect the abnormal behaviour based on Big Data. The proposed approach analyses faster and precisely various logs and monitoring data that have been discarded using Big Data storage and processing technology. In particular, we evaluated that the suspicious behaviour analysis using MapReduce is effective in analysing large-scale behaviour monitoring and log data from various sources.

**INNOVATING ADDITIONAL LAYER 2 SECURITY REQUIREMENTS FOR A PROTECTED STACK**

The OSI and the TCP/IP models divide computing communications into specific groups of activities that facilitate networking and communication. The models represent a theoretical and a pragmatic representation respectively of the systems and both provide security schema for protecting the services. In this exploratory literature research we asked; What are the security requirements for protection at OSI Layer 2? The hypothesis is that low level vulnerability adversely affects higher Layer security. The OSI model is selected to theoretically test the hypothesis and to answer the research question. The research shows that the precautions advocated in the OSI model are helpful but developing forensic capability and obfuscation further reduces the impact of unplanned events. A survey of attacks confirms previous literature that suggest Layer 2 has vulnerabilities and innovative solutions are required.
APPLYING MACHINE LEARNING TO OFF-LINK IPV6 HOST ENUMERATION

Conventional host enumeration strategies involve static processes for generating enumeration targets. These conventional host enumeration search methods include sequential and random distribution searches. Such strategies are appropriate for IPv4 host enumeration, however fall short when applied to IPv6 host enumeration. This paper presents novel host enumeration search algorithms that conduct dynamic searches of the IPv6 address space, to effectively locate networked nodes. Machine learning has been popularly used for exploratory research, however has not previously been applied to IPv6 host enumeration. The paper proposes an adaptive heuristic search algorithm and a genetic algorithm-based (GA) search algorithm that adaptively probes potential enumeration targets. Of the proposed algorithms, the adaptive heuristic search algorithm performed well, successfully probing 24% of one of the test datasets. The GA search algorithm failed to produce meaningful results when applied to the experimental datasets. With further refinements these novel search algorithms may provide more effective means for enumerating off-link IPv6 networks.

A METHOD FOR EVALUATING FUZZING TOOLS

Fuzzing is a software testing and vulnerability discovery technique that focuses on the systematic generation of test cases. Despite the widespread usage of fuzzing for the purposes of software testing and vulnerability discovery, a formal method for evaluating the relative performance of fuzzing software has not been published. This research was inspired by the inclusion of unjustified or potentially inaccurate comparisons of fuzzing tools in security and software testing literature. The aim of this study is to promote the development and usage of fuzzing tools of higher quality by producing a formally defined method by which fuzzing tools may be evaluated and compared to one another. Toward this goal, the potential evaluation methods of code coverage and simulated vulnerability discovery will be analysed to determine their effectiveness in accurately conveying the quality of fuzzing tools, with a brief discussion of the usefulness of retrospective testing for the same purpose. Two widely used fuzzing tools will be selected for the purpose of comparing the previously discussed evaluation methods. The fuzzing tools will be employed against common open source software containing known vulnerabilities in a test scenario. Code coverage data will be recorded from each test and subsequently compared to the number and severity of actual vulnerabilities discovered by each fuzzing tool. The usability and practicality of each evaluation method will also be discussed.

EVALUATING POLICY LAYER SECURITY CONTROLS FOR VALUE REALISATION IN SECURE SYSTEMS

A strategic question for any business is: What value do control frameworks give? The question concerns the costs associated with implementing and maintaining control frameworks compared with the benefits gained. Each control framework contains many controls that may or may not benefit a situation and this research is aimed at testing different selections and combinations of controls to forecast probable impacts on business outcomes. The scope of the research is limited to a representative set of security controls and the lessor question: What are the criteria for selecting the most effective and efficient security control configurations for best business value? We design a decision support tool (DSS), run a pilot study and begin to develop metric
process sets as part of the exploratory research. The conclusion is that in controlled environments the security controls may be optimised to deliver the best business value and that the highest performing sets of controls can be forecasted once the interaction factors are known.

LOYALTY CARDS AND THE PROBLEM OF CAPTCHA: 2ND TIER SECURITY AND USEABILITY ISSUES FOR SENIOR CITIZENS

Information Security often works in antipathy to access and usability in communities of older citizens. Whilst security features are required to prevent the disclosure of information, some security tools have a deleterious effect upon users, resulting in insecure practices. Security becomes unfit for purpose where users prefer to abandon applications and online benefits in favour of non-digital authentication and verification requirements. For some, the ability to read letters and symbols from a distorted image is a decidedly more difficult task than for others, and the resulting level of security from CAPTCHA tests is not consistent from person to person. This paper discusses the changing paradigm regarding second tier applications where non-essential benefits are forgone in order to avoid the frustration, uncertainty and humiliation of repeated failed attempts to access online software by means of CAPTCHA.

THE CHALLENGES IN IMPLEMENTING SECURITY IN SPONTANEOUS AD HOC NETWORKS

Mobile Ad Hoc Networks (MANETS) promise much in the ability to rapidly deploy a wireless network in a fashion where no prior planning is needed and the network can be running efficiently and with high security within minutes. Natural disaster response, military, education and business provide areas where MANETS can offer significant advantages in communication where infrastructure networks may take days to set up or may be impossible to implement. This research reviews a selection of MANET protocols to show the progression of the research and the issues that are yet to be addressed. It discusses the challenges to researchers in improving ad hoc schemes to the point where they work in theory and in practice. Areas are highlighted that pose the most significant challenges to developing new security protocols and some food-for-thought is given for those who wish to contribute to this growing area of importance for wireless communication.

SCADA SECURITY AND MODEL BASED IDS FOR MODBUS PROTOCOL

The proposed research will produce a framework for automated detection and testing of network borne malware threats that are present in industrial control systems or supervisory control and data acquisition (SCADA). ModBUS protocol is widely used on SCADA networks and other field devices and also used to control HVAC (Heating, Ventilation and Air Conditioning) and operational equipment such as industrial control systems. ModBUS protocol was developed and introduced in 1979 by Modicon. ModBUS is an application layer protocol and is used to transmit communications between master and slave. It was initially developed to provide reliability and availability however the security of the protocol and securing the infrastructure was not considered priority at the time. Therefore the industrial systems or infrastructure networks using ModBUS are increasingly insecure and exposed to a variety of cyber security attacks. The research aims to produce a framework or implement an IDS pattern using behavioural analysis of network of infrastructure systems using ModBUS protocol. The potential threats against ModBUS environment will be determined and the
behaviour of the threat on the ModBUS protocol environments will be analysed.

16th Australian Information Warfare Conference

THE SIGNIFICANT FEATURES OF THE UNSW-NB15 AND THE KDD99 DATA SETS FOR NETWORK INTRUSION DETECTION SYSTEMS

Nowadays, because of the increased overflowing of network traffics and its significance to the provision of ubiquitous services, cyber-attacks attempt to compromise the security principles of confidentiality, integrity and availability. A Network Intrusion Detection System (NIDS) monitors and detects cyber-attack patterns over networking environments. Network packets consist of high dimensionality (i.e., features/attributes) which negatively affects detection of anomalies. These features include some irrelevant or redundant features which reduce the efficiency of detecting attacks, and increase False Alarm Rate (FAR). In this paper, the feature characteristics of the UNSW-NB15 and KDD99 datasets are examined, and the features of the UNSW-NB15 are generated upon the KDD99 data set to identify the ability of these features to discriminate between normal and attack records. An Association Rule Mining algorithm is designed as feature selection to generate the strongest features from the two data sets. Some existing approaches are utilised to evaluate the complexity in terms of accuracy and FAR. The experimental results show that the original KDD99 attributes are less efficient than the generated UNSW-NB15 attributes from the KDD99 data set. However, comparing the two data sets, the accuracy of the KDD99 dataset is higher the UNSW-NB 15 dataset, and the FAR of the KDD99 dataset is lower the UNSW-NB 15 dataset.

THE CYBER SIMULATION TERRAIN: TOWARDS AN OPEN SOURCE CYBER EFFECTS SIMULATION ONTOLOGY

Cyber resilience may be characterised by an effects-based approach to missions and processes towards understanding and adapting to changing network conditions, including cyber attacks. One of the fundamental preconditions underpinning cyber resilience is an accurate representation of current network and machine states and what missions they are supporting. This research outlines the need for an ontological network representation, drawing on existing literature and implementations in the domain. This work then introduces an open-source ontological representation for modelling cyber assets for the purposes of computer network defence. This representation encompasses computers, network connectivity, users, software, vulnerabilities and exploits, aiming for interoperability with related representations in common use. The utility of this work is highlighted against a functional use-case depicting a realistic operational network and mission. Finally, a future research direction is defined.

IS INTERNET THE MAIN MEDIUM OF TRANSMITTING TERRORISM?

The developments of communication technologies which caused an influx of virtual media platforms have allowed extremists and terrorists to transmit their messages to wider audiences without passing through a gatekeeper or being a subject to editorial policies existed in traditional media outlets. Thus, extremists and terrorists exploit virtual media platforms to market their ideologies and report their actions, because it enabled them to have control over time and space to boost their objectives. As result, some governments tend to deprive extremists and terrorists from this 'oxygen' through monitoring the cyberspace
and blocking the suspected virtual media platforms. The extremists and terrorists' manipulation of virtual media platforms and the reactions of some governments to face this cyber invasion have shown that Internet is the main medium of transmitting extremism and terrorism. However, this paper debates this assumption, considering that Internet is just a medium to transmit extremism and terrorism, because heinous ideology and calling for violence are transmitted historically and still by other means of communication.

4th Australian e-Health Informatics and Security Conference

AUTONOMOUS DECENTRALIZED PEER-TO-PEER TELEMETRY AND ITS APPLICATION IN MEDICAL NETWORKS

With the advent of technology, the medical industry has been on the forefront of employing new technological advances in order to facilitate convenience for the masses at a marginal cost while still maintaining security, privacy, integrity and confidentiality. These considerations are of utmost importance as unlike other networks, the data or payload being transmitted in medical networks can have a life depending on it. In this paper we mention a few problems faced by the current type of network implication and focus on developing a new decentralized overlay system using the Blockchain to counter these issues. The network design proposed in this paper is a theoretical construct as of the publication of this document.

SECURITY RISKS OF MEDICAL DEVICES IN WIRELESS ENVIRONMENTS

The advancement of wireless medical devices technology, that has developed in hospitals and migrated into the home environment, has created unsustainability in in terms of the management of security for such devices. Through this paper, we shall attempt to explain how medical devices have completely changed the way security needs to be approached in the medical field. We shall also explore the history of medical devices and the organizational problems faced for the development of these devices, the different stakeholders strengths and weaknesses, especially if the device is implanted inside the body of a patient. Once the risk is understood we can then endeavour to mitigate it. We shall also explore how we can put in place a system of prioritization of medical devices that will enable us to reduce the risk threshold for our medical devices.

SECURITY OF EPRESCRIPTION: SECURITY OF DATA AT REST IN PRESCRIPTION EXCHANGE SERVICES VS ON MOBILE DEVICES

One area of healthcare that has moved more quickly than others in adopting electronic transfer of information is prescribing in the primary care environment. Several Acts and Regulations have been repealed and amended at Commonwealth and State levels to enable this progress over the past decade, as medication provision is a strictly controlled area of healthcare. Further, numerous standards and specifications have been developed and adopted to support and safeguard the regulatory changes and facilitate the electronic transfer of prescription. However, the current model of electronic prescription transfer comes with a substantial price tag for use with an associated ongoing cost for every electronic prescription downloaded. With the Nation’s growing population, particularly with an aging population, the number of prescriptions will increase in the years to come and thus it is necessary to explore more cost-effective alternatives with comparable security and privacy assurances. The first potential candidate identified in this exploration are devices that have been a part of our daily lives for well over a decade - mobile smartphones. Consequently,
a thorough investigation to determine whether or not such technology is capable of meeting prescribing legislation whilst providing a cost-effective alternative to our current expensive electronic prescription transfer model. The investigation established that although the proposed alternative is not a flawless one, it also opens up opportunities to incorporate many useful features in addition to eliminating the associated on-going costs while providing comparable privacy and security assurances.

8th Australian Security and Intelligence Conference

EFFICACY OF PROPERTY MARKING AS A SITUATIONAL CRIME PREVENTION STRATEGY

Burglary and stealing are crimes that have a significant impact and cost on its victims and society. To mitigate such crimes, property marking is a situational crime prevention strategy that attempts to prevent through dissuasion. There are many forms of property marking, yet there is limited research of its efficacy. Where there have been such studies, there has been some indications of success. Therefore, the study assessed the efficacy of property marking to reduce burglary and stealing crimes. The study undertook a quantitate approach using non-equivalent control groups to assess the geo-spatial impact of property marking when applied at a saturation level. Three housing groups were established (N878), comprising an experimental (n278), adjacent (n300) and control (n300, group, with significance measured using a Wald Chi-square method. Results indicated that when property marking is applied at saturation levels (≥80%), both burglary and stealing crimes decreased significantly. Furthermore, that displacement for both burglary and stealing occurred in the adjacent area. Recommendations suggest that property marking should not be used in a sporadic manner; instead, targeted at an optimal saturation level. Such targeting should have the aim to target burglary and stealing hotspots and saturate these areas for property marking to work effectively.

CREATING AN OPERATIONAL SECURITY MANAGEMENT STRUCTURE FOR INIMICAL ENVIRONMENTS: PAPUA NEW GUINEA AS A CASE STUDY

Security is a necessary cost for businesses wishing to operate in the developing economy of Papua New Guinea. The country continues to face levels of crime and violence out of proportion to other East Asian countries; which deters many would be investors. However, the potential in PNG is vast and eagerly sought after despite the high costs required to operate without harm, therefore, it is necessary manage the security situation. Experience from similar countries has shown by using optimal security management systems and structures it is possible to work safely, securely and effectively, but this requires a comprehensive security, threat and risk assessment to be conducted first . Based upon this assessment, a security management plan can be created . The predominant threat comes from criminality, which is endemic in parts of PNG. The police force is struggling to address the issue, but due to lack of resources and manpower is often seen as part of the problem. An inimical model is therefore proposed that incorporates the local community and actively seeks their support to gather greater intelligence to thwart would be criminals. In addition, empowering more local security managers, with their vital local knowledge, will improve the overall intelligence flow.
What you can expect at the 2015 SRI Security Congress
November 30 - December 2, 2015
Perth, Western Australia

UTILISING SMALL DRONE SURVEILLANCE CAPABILITIES TO ENHANCE TRAFFIC CONFORMANCE INTELLIGENCE

The availability of cheap small physical drones that fly around and have a variety of visual and sensor networks attached invites investigation for work applications. In this research we assess the capability of a set of commercially available drones that cost less than $1000. The assessment reviews the capability to provide secure and safe motor vehicle surveillance for conformance intelligence. Trials were conducted and the results reported. The conclusion is that more than $1000 needs to be spent on the drone and the resources for effective observation but less than $3000 in total is sufficient for the work application. The result and the analysis of traditional surveillance networks suggests that such drones can provide a low entry risk for additional benefits; and intelligence to those responsible for compliance on our roads.

CCTV SURVEILLANCE: THE DIFFERING AIMS AND FUNCTIONS OF CCTV WITHIN THE CORPORATE STRATUM

Closed Circuit Television (CCTV) systems are found in a variety of environments and used for a multitude of purposes, leading to differing views of CCTV within an organisation. In accordance to management theory, organisations contain a stratum of work where each level requires specific skills set. In accordance with this work stratum, the study’s methodology used semi-structured interviews with different levels of security personnel in a Casino complex to extract and undertake a thematic analysis. The study extracted 10 CCTV surveillance features across two themes, being its aims and functions. CCTV features included creating a safe environment, protection, legal compliance and audit, management and support, deterrence, investigation and evidence, all of which were considered at each stratum levels; however, with difference in their meaning. Recommendations suggest that articulating clear awareness of CCTV aims and functions across the corporate work spectrum would result in a more effective CCTV surveillance system.

ATTRIBUTES OF AN ANALYST: WHAT WE CAN LEARN FROM THE INTELLIGENCE ANALYSTS JOB DESCRIPTION

Intelligence is a function embedded in the organisational structures of government agencies and departments at the federal, state and local level. The intelligence analyst plays an important role in supporting the operational and policy decision makers in those organisations. Notwithstanding that important role, there has been limited research into the attributes of good analysts. In the course of this research we examined 300 advertised analyst job descriptions and compared the attributes sought with those attributes described in the literature. Whilst some correlation was identified, the generic nature of the attributes sought suggests that it may be possible they have a negative influence on the quality of candidates applying for the roles. This research is significant in that it suggests that organisations and departments may need to rethink the construction of the analyst job description.

DOES A WEAK SECURITY DISCOURSE PROVIDE OPPORTUNITY FOR SECURITY DEVIANCE TO FLOURISH?

In the years since the tragedy of 9/11 the term “security” has become a much used and abused term. As the war on terrorism has evolved politicians of all persuasions played the security card to change law and legislation ostensibly to protect the community. Those whom provide the security assume that freedoms lost by the
wider community in the name of security are in fact a fair price to pay for that security. In this environment the security discourse is diminished and this provides an opportunity for security deviance to emerge. This research used a selection of publically reported examples of security misconduct to examine and define the construct security deviance.

FORMATION OF THE RADICAL SELF: CONSTRUCTS OF CHANGE IN WESTERN YOUTH TO ACTS OF TERRORISM ON HOME-SOIL

The terrorist attack on a member of the Police service by a 15 year old boy in late 2015 sent shock waves not only through Australia but also throughout the world as the realisation of Islamic State targeting teenagers becomes a reality. This paper uses a blend of theoretical and empirical evidence to examine how the radicalised self is formed. Insights from various frameworks including: developmental psychology (teenage identity formation and role confusion), Foucault’s technologies of the self, governmentality and sociological issues including the perceived gap between Muslim values and those of the West. Coupled with these theoretical frameworks are empirical insights including the use of grievances and key discourses, radicalisation material as well as the use of future pacing strategies to embed change to acts of violence. Ultimately, recruiters aim to take advantage of teenage identity issues as well as marginalised individuals to help construct a radicalised youth prepared to undertake acts of terrorism on home-soil.

SYMBIOTIC RADICALISATION STRATEGIES: PROPAGANDA TOOLS AND NEURO LINGUISTIC PROGRAMMING

The rise of Islamic State has seen a rise in the threat and incidences of domestic terrorism. Sophisticated strategies are being used to target youth and draw them into the ideology of Islamic state and other terrorist groups. Two common strategies used by Islamic State are the use of propaganda tools as well as Neuro linguistic programming strategies. This paper looks at how these strategies were used through a longitudinal online ethnographic study on the social media site Facebook. Data collected revealed that these two strategies were used in a targeted manner and worked together in a symbiotic fashion to create a change in the mental frameworks of an individual. Both strategies worked in the linguistic domain to help shape and internalise key discourses and ideologies. Finally, these strategies were used implicitly without any direct references on how to achieve change.

INSTITUTIONALISED MORAL REFRAMING: A RESEARCH BASED MODEL ON ISLAMIC RADICALISATION ON SOCIAL MEDIA

Institutionalised Moral Reframing is a new research model on Islamic radicalisation based on on longitudinal ethnographic research on social media. Prior to introducing the model, an overview of other radicalisation models will be presented with a brief overview of each. Critical to the Institutionalised Moral Reframing model is the concept of socialisation via an online institution of social media where an individual is isolated from competing discourses. The model uses two axis, a moral authority axis and a moral discourses axis. These two axis are mutually reinforcing and enable an individual to progress along stages in a context that includes multifactorial bubbles which encapsulate the many factors responsible for an individual’s radicalisation.

VIOLENT-EXTREMISM: AN EXAMINATION OF A DEFINITIONAL DILEMMA

This article aims to demonstrate how radicalisation, violent-extremism and terrorism are terms often used interchangeably – terms
that do not have the same meaning and are generally poorly defined. It will reveal, as with other terminologies pertaining to this area of interest, how violent-extremism has no universally accepted definition, and how it remains tainted with ambiguity. Arguably, the term is predominantly used as a social label in discussions on terrorism and other forms of extreme violence — particularly applied to those who have a distorted interpretation of religious ideology to justify the use of violence to achieve specific socio-political goals.

To provide a better understanding of violent-extremism, its root causes and its prevention, a proposal of an accurate depiction of its meaning and clarification on the context of its use is paramount. This article will provide a brief introduction to the terms radicalisation, violent-extremism and terrorism; and present various ways in which they have been defined in existing academic literature and policy documents. It will further explain the delineation between the three terms; and propose a practical definition for the term violent-extremism to enhance our ability as a community to apply appropriate measures to prevent escalation of root-cause issues that potentially lead to violent action.

A SECURE SHARING DESIGN FOR MULTI-TAG RFID AUTHENTICATION PROTOCOL

In recent years, RFID technology has been increasingly used in supply chain management due to its great offer in providing accurate information, easiness control and reducing labor cost. These advantages have taken place by using RFID in supply chain management (Masum and Bhuiyam, 2013). Although RFID can enhance the efficiency of supply chain management, there are also some issues that have to be considered such as scalability and security challenge. RFID based solution have been developed. However, they do not address a number of risks related to security and privacy of the information that is stored in each tag, e.g. unauthorised reader can read the information inside the tag, illegitimate tags or cloned tags can be accessed by reader that generate privacy and security problem. Also, most of authentication protocols still focus on single reader and single tag authentication. This paper seeks to propose an authentication protocol that allows sharing the encryption message with multi-tag during the authentication process. The proposed design points out the idea of combining the lite version of Cramer-Shoup cryptosystem with the Shamir’s secret sharing scheme. This combination allows sharing the encrypted message within multi-tag and managing up key distribution during the authentication processes. The security and privacy of the proposed protocol insures by the property of the lite version of Cramer-Shoup which is secured against non-adaptive chosen cipher-text.