

INFORMATION WARFARE: COMPUTER NETWORK DEFENCE STRATEGIES

By

Ron Brandis, Rob Webb and Albert R. Zehetner
Electronic Warfare Associates – Australia
Canberra, Australia
www.ewa-australia.com

“Information operations integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battlespace at the right time, at the right place, and with the right weapons or resources.” [1]

Abstract

The current threat of Information Warfare (IW) is directed not only at military forces combating a known foe but towards society as a whole. The IW threat is asymmetric in nature with adversaries ranging from nations to non-state-actors; from primitive technology groups to sophisticated cyber criminals; from open IW offensives to clandestine attacks.

The impact of IW reaches further than just at government and military forces. Society as a whole, due to a dependency on critical national infrastructures and other communication media we take for granted, are and can be targets. A wide range of industries across both the private and public sector are being attacked on a daily basis by a variety of hostile parties. The information conduits we use everyday are no longer secure – our computing networks are vulnerable. There are, however, strategies to address information protection.

This paper describes network vulnerabilities and provides an understanding of Computer Network Defence (CND) Strategies that seek to safeguard against attacks.

Dependency on technology

Society is dependent on critical national infrastructures and other communication media, including public utilities, banking and finances, health, national security and private enterprises. This dependence on infrastructure and communication is reflected in military environments. With the need for any commander to react to an incident and make their decisions based on sound and timely information, they require access to many systems and connection to other teams to enable interoperability. However, it is this interconnection that may expose the vulnerabilities of some of these systems to attack.

Information systems are developed using various components, which we generally trust and believe

have been thoroughly tested – is this a false sense of security?

For example, a developer designing a system to the requirement, “*this system requires a secure connection*”, may utilise a Secure Socket Layer (SSL). They may use the Microsoft SSL package; however a recently announced vulnerability within this component would render the system vulnerable.

Our dependency upon technology has also raised expectations that we will be able to access our information systems anywhere, at any time. The most recent Gulf conflict demonstrated how reporters deployed with front line troops could relay news stories instantly back to anywhere in the world, as well as to any person with a device such as a PDA or mobile phone. What about that young trooper who connects their PDA to their combat system – even though it is against the rules? This may result in an unknown and uncontrolled connection to the Internet.

Threats to information

Security of information and assets is built around the three main principles of ensuring the integrity, confidentiality and availability of information systems. A threat to any one of these aspects may put the entire system at risk.

It is commonly accepted that sources of threat to a system arise through the actions of:

- Internal staff
- Contractors
- Former staff and contractors
- External service providers
- Other interested parties – hostile countries, rival companies
- Hackers / vandals
- Natural sources

Many security measures are aimed at defending systems and infrastructure against attacks from these threat sources. In addition, consideration should be given to vulnerabilities inherent in the systems or applications themselves, which an

[1] Frater, M. and Ryan, M. (2001), *Electronic Warfare for the Digitised Battlefield*, Artech House, Norwood

attacker could exploit to successfully compromise a system.

Systems are generally made up of a number of components (applications/processes), some developed within an organisation and others, such as the operating system itself, supplied by third parties, e.g. Microsoft. Vulnerabilities or weaknesses present in various components, can lie dormant until detected.. When detected, attackers can examine the vulnerability for a successful exploitation that can be used to threaten or compromise the host system/application or other systems.

A system can be a threat source to an application, or an application can be a threat source to a system.

A vulnerability (weakness) provides the opportunity, through changing the state of a system (application) allowing the compromising of integrity, confidentiality or availability of a system or its data.

Common vulnerabilities in today's information systems include:

- information leakage;
- vulnerabilities existing because of poor coding practices;
- misconfiguration of systems/applications; and
- lack of information security awareness

This paper discusses the first two forms of common vulnerabilities.

Information leakage In a military situation, commanders in the field conduct reconnaissance missions against the enemy to gather information about them to determine vulnerabilities which may be exploited. The same approach is adopted within the IW field.

Attackers can perform passive and active forms of reconnaissance. Active reconnaissance is where the attacker directs their efforts at a target's systems through various types of probes and scans. This is to identify system types and the services being provided or allowed to be connected to within those systems.

Passive reconnaissance is where the attacker attempts to collect information about the target in a jig-saw fashion. Information gathered may include associations of the target (vendors, server providers), the types of systems and software the target uses, their modes of network access and current security standing. As this information gathering is conducted through open source searching, the target will be generally unaware of these probes.

An attacker will compile a description of the target, develop an attack plan based on this description

and assess the chance of a successful attack. If the likelihood of success is high then the attack may be undertaken. Having found a vulnerability to exploit, the attack itself may simply involve the attacker identifying and deploying the appropriate tool.

Vulnerabilities that exist through information leakage provide useful information to an attacker. As with any form of intelligence, the control and containment of information is key to a successful defence. With today's technology this becomes very hard to achieve, partly because many information systems users and administrators are unaware of the various sources that may reveal useful information including the Internet, newsgroups, vendor sites, and the target systems themselves.

An example of this is the many applications that display the version and patch level numbers through banners. If an attacker can identify that an application version is 1.x and this version is currently exploitable, they may have an easily exploitable target.

Another example of information leakage is through various Internet newsgroups. A system administrator trying to solve a problem may post to an internet newsgroup requesting help: *'I am having problems with users connecting to our Cisco VPN v3.2.1 connection, through out Checkpoint firewall v4.1.1- what policies should I setup?'*. Such a posting provides a wealth of information to a potential attacker.

A www.google.com search under groups with the search string 'firewall help' in May 2004 returned more than 598,000 results. A veritable feast of information for attackers! A search using 'firewall help .mil', returned 4,210 results from the US military, who perhaps should be more aware of security, than the general Internet user.

In many cases, information leakage in itself may not directly enable an exploit of a target (unless the complete network and passwords have been posted to the network, which I have seen happen).

Poor coding practices The most common examples of poor coding vulnerabilities are 'input validation' and 'buffer overflows (BOF)'.

Input validation vulnerabilities exist due to poor development of an application. In vulnerable systems, data sent to a server is not fully validated, or checked as this functionality is presumed to be completed on the client. Hence, an attacker can circumvent the client and compromise the server directly.

Examples of this include:

- hidden field changing - manipulating web pages via unanticipated input to control or manipulate the application, and
- SQL injection - injecting SQL database commands to the SQL database server that can be used to control back-end systems.

Buffer overflows have been around since the 1970's and are also due to poor coding. Buffer overflows occur due to an application only being able to handle a certain amount of input. By sending more input than is expected an attacker can force the application into an un-controlled state. The attacker's payload can then change the state of the target system to perform commands the attacker transmits.

Table 1 illustrates recent Microsoft-discovered input validation and buffer overflow vulnerabilities. These can make any Windows operating system vulnerable and exploitable - the most threatening, discovered in April 2004, is that any system built or using Microsoft's Secure Socket Layer (SSL) can now be compromised and controlled. Today, many of the worms that are released onto the Internet simply automate the basic vulnerabilities

as shown in Table 1.

The information in this table demonstrates that threats to a system and network can be introduced by a system's trusted components.

The significance of these threats in an Information Warfare context

Historically the military has maintained security through rigid access controls — only those with the need to know have had access. This made compromise of these systems difficult, and it was usually only achieved through deliberate acts on behalf of the perpetrators. These systems were usually stovepipe in nature – they were not connected to other networks or systems. Such systems are now considered inadequate in providing information to those that require it in a timely manner. These systems are also cumbersome in reacting to any compromise, resulting in significant down-time whilst the organisation and system recover.

With the advent of Internet technologies, traditionally segregated classified systems are more and more sharing infrastructure with unclassified systems. This increased connectivity means that many persons now have some form of access to previously isolated systems. This widespread access increases the likelihood of the system being compromised, possibly with catastrophic effects. For example, compromising a supplier could result in logistic requirements being changed delivering the wrong supplies and thus debilitating the fighting force, through to false intelligence information resulting in the destruction and possible deaths of non-combatants and non-military installations.

A Computer Network Attack (CNA) aims to coordinate, support and conduct computer network attack operations in an attempt to investigate, breach or otherwise compromise target information systems. It includes any activities designed to disrupt, deny, degrade, or destroy information systems and computer networks.

Many attacks do not target an information system directly, but focus on attacking other related systems with a view to controlling the infrastructure that surrounds the target system.

Industry has been quick to leverage off the latest technologies, and nowadays most essential services from electricity to ambulance services utilise information networks to provide and monitor services. Compromise of such systems can be debilitating to a country or region.

Table 1: Some Declared Microsoft Vulnerabilities [2]

Microsoft Component	Impact of Vulnerability	Windows NT 4.0	Windows 2000	Windows XP
LSASS Vulnerability (BOF)	Remote Code Execution	None	Critical	Critical
LDAP Vulnerability (BOF)	Denial of Service	None	Important	None
PCT Vulnerability (BOF)	Remote Code Execution	Critical	Critical	Important
Winlogon Vulnerability (BOF)	Remote Code Execution	Moderate	Moderate	Moderate
Metafile Vulnerability (BOF)	Remote Code Execution	Critical	Critical	Critical
Help and Support Center Vulnerability (poor validation)	Remote Code Execution	None	None	Critical
Utility Manager Vulnerability (poor validation)	Privilege Elevation	None	Important	None
Windows Management Vulnerability (poor validation)	Privilege Elevation	None	None	Important
Local Descriptor Table Vulnerability (poor validation)	Privilege Elevation	Important	Important	None
SSL Vulnerability (BOF)	Remote Code Execution	None	Critical	Critical

[2] www.microsoft.com/technet/security

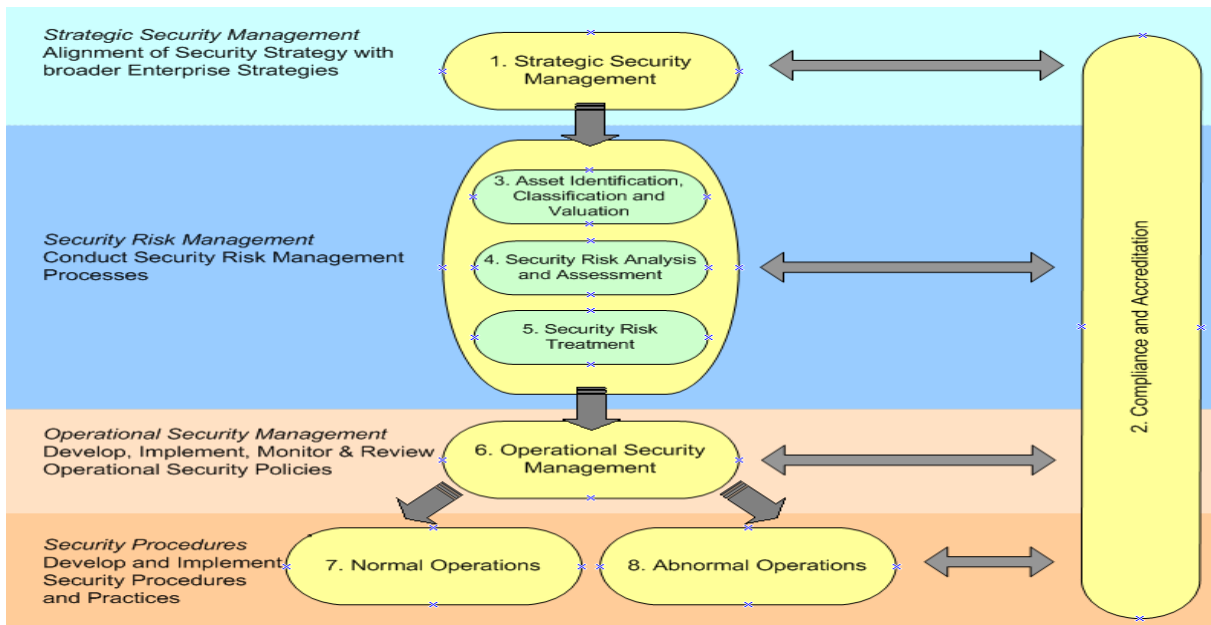


Figure 1: EWA's Security Methodology Approach

The MSBlast Worm is thought to have been one reason for a major power failure on the east coast of the USA, as reported in 'Internet worms and critical infrastructure, December 9, 2003'.^[3] This incident demonstrates the possible consequences of a loss of services.

Transport infrastructure, including airlines, are also susceptible to attack with significant consequences. In May 2004 flights from Heathrow International Airport were reported to be delayed after a computer virus crashed software at British Airways check-in desks. The Sasser worm, which spreads through the Internet, is also reported to have affected check-ins operated by US airline Delta.^[4]

During April 2003, a rumour started on a Web site that Bill Gates had been shot dead in Los Angeles. It was then broadcast over South Korean TV and other networks causing share prices on the South Korean stock exchange to slump as panic selling ensued. Shares fell by 1.5% and were set to slump further until Bill was found alive and well.^[5] This is essentially a modern form of the WWII propaganda broadcaster Tokyo Rose concept, but far more effective with our current reliance on technology and communication media.

Commercial companies, including suppliers to services to defence, such as Microsoft have been hacked and versions of yet unreleased code have been downloaded. Attackers also target application developers' systems, with the intent to install malicious code within a program before it is commercially deployed.

A common attack today is to compromise a home computer, easily done through a buffer overflow

exploit (see Table 1), and via the compromised system direct attacks at the intended target, or even more creatively, compromise another weak system and launch attacks through a chain of controlled systems. If these weak systems are those of the governments of another country, it may appear that the IW attacks are coming from those governments.

These examples illustrate the far-reaching effects of Computer Network Attacks in both the military and civil fields.

A Security Framework for Computer Network Defence

Computer Network Defence (CND) describes the actions taken to protect, monitor, analyse, detect, and respond to unauthorized activity within information systems and computer networks. CND protection activity employs information assurance principles and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information.

There is no 'silver bullet solution' for information security. Instead a robust, flexible and living Security Framework methodology should be developed and tailored to meet individual and organisational security requirements.

The ever increasing complexity and functionality of software applications has driven an unfortunate and alarming trend from threats to exploits. Adopting a Security Framework is a solution that will help identify and manage risks to organisation.

Figure 1 illustrates EWA's Security Methodology approach to provide a comprehensive set of processes to assist organisations build

[3] www.news.com

[4] www.raes.org.uk

[5] www.theinquirer.net

applications and systems by enabling secure use of the Internet or other networks.

Investigating and implementing core security concepts helps achieve a specific security posture that reflects the security needs of an organisation. Examining an organisation's process areas and functional disciplines in relation to Information Security can aid this and later processes. The process areas that comprise a strategic security framework are:

1. Strategic Security Management – providing leadership, coordination alongside the establishment of organisational goals, policies and legislative requirements.
2. Compliance (Standards/Legal) – the monitoring, review and auditing of the organisation's information systems to ensure that legal, national and organisational requirements are met.
3. Asset Identification, Classification, Valuation – understanding what requires protection and the degree of protection required.
4. Risk Analysis and Assessment – assessing the existence and extent of a specific risk or threat.
5. Risk Treatment – the development and recommendation of treatment options for identified risks.
6. Operational Security Management – managing the daily operation of information security.
7. Security Controls in Normal Conditions – risk countermeasures operating in normal day-to-day conditions. (Proactive measures – Protection and Detection)
8. Security Controls in Abnormal Conditions – preparations for maintaining information security in adverse conditions, eg a natural disaster (Reactive measures).

Functional Disciplines can include:

- Theory – theoretical information.
- Environmental and Infrastructure Security – services the organisation is dependant on, eg banking, water, power, etc.
- Systems Security – Server, operating system, and software security. Includes software development.
- Communications and Network Security – Firewalls, routers, comms and network design.
- Physical Security – doors, cards, fences, gates, cameras, guards, etc.
- Personnel Security – issues directly related to an organisation's staff, eg dismissal procedures, theft management, etc.

Strategic Security Management

Before committing a Security Strategy, the executive must support and endorse the requirement for this strategy. This process involves the following:

- Defining organisational governance;
- Identifying relevant legislation as it applies to the business;
- Identifying information that the business needs to create and consume;
- Aligning security mission, goals, objectives (organisational strategy)
- Identified required security policies; and
- Communication and ownership of the security strategy.

The outcome of this process provides the highest level of ownership and guidance for the continuation of the security process and development of the security framework.

Asset Identification, Classification, Valuation

The strategic guidance provided by management will assist in the identification, classification and valuation assets as viewed by the organisation. Assets can be equipment and facilities, intellectual property (data, knowledge, procedures), even staff and reputation. The classification and valuation of the assets is usually rated by the effect (monetary) of their compromise or failure.

The outcome of this process is an asset register aligned with executive guidance which forms the basis for the Threat and Risk Assessment.

Threat and Risk Assessment

The aim of this step is to generate a comprehensive list of threat sources and threat events, against the assets identified, that may affect the organisation as well as identify possible causes and scenarios for each event. The use of a systematic process to identify potential security threats relevant to the organisation is critical. This process should assess the relevant security threats to the organisation based upon identification and evaluation from both a business and technical perspective.

In identifying risks, it can be useful to consider the potential Threat Source, their resources and knowledge, motivation and incentive, and past activities.

A threat event is the scenario in which a threat source can attack an organisation's assets. A threat event can include, but is not limited to:

- Damage/disruption to communications paths,
- Theft or damage to equipment,
- Software/hardware failure,
- Natural or environmental disaster,
- Denial of service attack,
- Malicious code infection, and
- Abuse of privilege by staff.
- Performance measurement against specified criteria,
- Monitoring and review requirements, and
- Assessed residual risk after treatment.

The next step is to identify the existing management, technical systems, and procedures to control risk and assess their strengths and weaknesses. This should be conducted in accordance with AS/NZS ISO/IEC 17799. A variety of tools can be used to determine the existing controls including:

- Review of documentation,
- Judgments based on experience and records,
- Flow charts,
- Brainstorming, and
- Systems engineering techniques.

Having identified and analyses possible threats and risks, it is necessary to assess the consequence and likelihood in the context of the existing controls. Consequences and likelihood may be determined using statistical analysis and calculations. To avoid subjective biases the best available information sources and techniques will be used when analysing consequences and likelihood. Sources of information to be used include the following:

- Organisation records,
- Relevant experience of the organisation,
- Industry practice and experience including CERT Computer Crime Survey results,
- Relevant published literature, and
- Specialist and expert judgements.

Risk Treatment

The outcomes of the Threat and Risk Assessment are the major inputs into the risk treatment process which should result in a Risk Treatment Plan. This plan includes:

- Identification and assessment of risk treatment options for each identified security risk, options include risk avoidance, transferral, mitigation or retention.
- Responsibility and accountability for implementation of the risk treatment plan,
- Timeline for implementation of the plan,
- Resources requirements,

In combination, the above tools provide a sound basis for security design of systems that will assist the system user and support staff achieve the IA requirements they desire. There are a number of known controls that can be put in place to mitigate the risks that have been identified that impact on the Organisations system. Some of these control mechanisms are outlined below:

- Disaster recovery planning. Specific plans made to ensure continuity of IT services in the event of a major disaster or catastrophe;
- Access controls. Measures that ensure that persons have access to only those system resources and information for which they are legitimately authorised;
- Security policy and procedures. Documented policy and processes relating to the desired secure operation of the system;
- Audits. Third party assessments against defined criteria to ensure the system is operating as intended;
- Infrastructure monitoring. Monitoring the state of system components using both manual and automated means;
- Intrusion detection systems. Automated systems that constantly scan for system behaviour that matches known intruder actions;
- Audit logs. Records of system events, written as the events occur
- Outgoing connections only. Only outgoing connections from the network will be allowed;
- Security education and awareness. Knowledge and awareness of operations and security by all stakeholders;
- Physical security. Physical segregation measures taken to restrict access to system hardware;
- Hardware spares. Spare hardware kept for the replacement of failed components;
- Environmental controls. Environmental maintenance equipment and design, such as air conditioning and fire suppression systems;
- Regular software patching. The application of software patches to ensure that known system vulnerabilities are addressed;
- Firewall. Network traffic filter designed to prohibit unwanted or disallowed network packets;

- Replication of hardware and system components. Having more than one of each system component operating at a time, such that if one component fails, service is maintained by the other;
- Anti-virus software. Software designed to detect, quarantine, eliminate and report on malicious software found with the system

Operational Security Management 'Making it work'

Operational Security Management: implements and monitors the controls required to achieve the required level of information assurance defined in the previous steps and endorsed by management, adding specific operational details. Whilst commonality in the use of terms is important, the ultimate goal is to ensure there is a clear understanding of roles and responsibilities at both the strategic and operational levels and effective communication mechanisms between these organisational levels. These processes must include such things as configuration management, change management, incident response, auditing etc. These can be further defined as Normal operating procedures and Abnormal operating procedures.

Security Controls in Normal Conditions

Before the abnormal can be readily identified, 'normal operations' for an organisation must be defined. For most organisations, this is not an issue. Daily practices, as defined in operational procedures, should identify most normal conditions. These may then be supplemented with additional data obtained from employees, regarding normal activities. Events occurring during normal conditions are often written up as procedures and meet specific policies or standards.

Once we know the actual norm, it is also possible to define what the desired norm would be. By no means does this need to be a formal process. Simply, it is a good idea to know what is normal, so that the abnormal is more readily identified.

Examples of "normal" procedures include software updates, change control and backups.

Security Controls in Abnormal Conditions

Abnormal conditions or operations are defined as being those conditions that occur outside of the realm of normal conditions.

Whilst Abnormal Conditions normally related to an 'incident' and operate outside of Normal Conditions, it does not follow that abnormal

conditions are not proceduralised or planned for. Indeed in a well-structured organisation, they are often planned for and proceduralised to some degree.

Examples of "Abnormal" procedures include Business continuity plans, Disaster recovery plans and incident response.

The outcomes from the operational Management components result in a snap shot status of the security of the system as it is currently, and a recent history of events relating to the system.

Compliance

Within the framework of layered security, compliance:

- Helps provides a first layer of defence for the organisation from security threats.
- Highlights obligations and responsibilities – which raises the overall security posture of organisations – weak legislation will mean a weak security consciousness and environment
- Provides a deterrent for would-be attackers – illegal activity can lead to prosecution.

Most importantly compliance allows an organisation to verify that the security requirements of the organisation are being correctly addressed through physical implementation and / or procedures, and hence supporting the business objectives of the organisation. That is, there security framework is relevant and active. Methods and procedures to ensure compliance of security regime with international, national and industry standards and guidelines as well as legislation include:

- Seeking advice from Legal Council.
- Audits and reviews (refinement lifecycle).
- Quality control
- Establishing, maintaining and enforcing legally sound procedures.
- Employee education and re-education.

The security management process described assists organisations in developing; implementing and maintaining their required security framework and as a result, achieve the desired security posture. There are a number of Security framework guides around including:

- ISO/IEC 17799 – Information Technology – Code of Practice for Information Security Management allows

- for a comprehensive security assessment; and
- ISO/IEC TR1335 – Information Technology. Guidelines for the management of IT security.
- Common Methodology for Information Technology Security Evaluation CCIMB-2002-07-001 Supplement: Vulnerability Analysis and Penetration Testing provides a means of verifying the security of the system through vulnerability assessments and penetration testing.

Information Risk Management methodologies are based upon a broad range of national and international standards including, AS/NZ Standard 4360 – Risk Management, AS/NZ Handbook 231 – Information Risk Management and AS/NZ Handbook 240 – Guidelines for Managing Risk in Outsourcing.

New Zealand Standard 4360:1999 Risk Management contains seven stages. These stages are:

- Communication and consultation;
- Establish the context;
- Identify security risks, (Asset, Vulnerability and Threat Assessment);
- Analyse the risks, (Likelihood, consequence and existing controls);
- Evaluate the risks (Assessment and Prioritisation);
- Treat the risks; and
- Monitor and review.

Most importantly a security framework adopted by an organisation must demonstrate flexibility. Every success in defending systems from attack may result in a new counter attack. A security framework must allow for proactive action to maintain the required security posture.

Summary

Applications can threaten systems because of vulnerabilities inherent in them due to poor coding practices and because developers may have a limited understanding of attacks. We've presented a Security Methodology approach that can assist organisations in building complex applications and systems. The outcomes of the various processes are validated, ensuring compliance with the overall business goals.

A framework is used within this Security Methodology, that if applied throughout all stages of the application development life-cycle, would help identify, manage and reduce (but not remove) threats and risks.

Authors' Biographies

Ron Brandis MIT BSc CISSP is a Senior Information Security Consultant at EWA-Australia. Ron has held a variety of Information Security consultant and development roles in both the public and private sectors, notably with the Department of Defence and the intelligence community. Ron's expertise lies in risk, threat and vulnerability assessments of applications. He has conducted numerous vulnerability and penetration tests for clients ranging from small businesses to international organisations, in both the public and private sectors. Ron has also provided hands-on InfoSec training for clients, including law enforcement personnel, in hacking techniques.

Email: ron.brandis@ewa-australia.com

Rob Webb MSc(IT), BEng Computer Systems. Rob is currently a Senior Information Security Consultant with EWA-Australia. Rob has managed the development and implementation of many security related communications and information projects.

Email: rob.webb@ewa-australia.com

Albert Zehetner MSc ME BE CEng MRAeS manages EWA-Australia's Information Security Group and has been involved in EW and C2 military systems engineering projects, network and application information security activities. Prior to joining EWA, Albert was employed in the Australian Defence Organisation in a number of roles including engineering manager of a major capital acquisition project, airworthiness regulator, and tactical fighter ILSM at RAAF Williamtown.

Email: albert.zehetner@ewa-australia.com

*Electronic Warfare Associates – Australia
Canberra, Australia
www.ewa-australia.com*