Technical Evaluation Report

Glyn Wyman
United Kingdom

INTRODUCTION

This report addresses the IST -111/RSY-026 symposium on **Information Assurance and Cyber Defence** held in Koblenz on 24th September 2012 and 25th September 2012.

Information Assurance and Cyber Defence is an essential element for the modern war fighter and is an important theme within IST and clearly aligns with hard problem 9 in the RTO/CTO report. This was the latest symposium of a series and inter alia exposes some of the work of the task groups sponsored by IST. The subject is also important in a wider context because of the potential impact on Governments and the general public.

The increased use of IT and the desire to have information readily available places demands on the infrastructure and exposes weaknesses which can be exploited by third parties. Progress in this discipline is driven, primarily from civilian aspirations with the inherent relaxed specifications. The aim of the symposium was to provide a forum to exchange relevant knowledge associated with Information Assurance. It is recognised, however that availability, integrity and confidentiality of data particularly within a coalition network is challenging. The 'Call for Papers' identified 24 topics and from the abstracts received the Technical Committee grouped the select 23 papers into six session (MANETS and Sensor Networks was subdivided each with its own chairs). The topics selected were relevant and covered a broad spectrum incorporating, to some degree, those raised in the call for papers.

Perceived Military Issues

Any decision is only as good as the inference which is drawn by the decision maker from his background knowledge and the information presented. This will be coloured by confidence in the basic data; identified by the level of assurance and the belief that the source and the intervening media has not been compromised or contaminated. Adversaries are constantly evolving new methods and modifying existing techniques to disrupt or deny the smooth flow of information.

The move towards cyber terrorism is inevitable with the general public unknowingly hosting malware which could be exploited by a bothandler. Infiltration of military nets follows made easier if military systems are based on commercially available software. A large number of incidents are regularly reported. An attack could take a generalised form or an ad hoc attack on a specific entity. Defence is required across a broad front involving many disciplines. Once malicious code has been identified trained staff are required to undertake the reverse engineering role to devise the counter. Indications are that engineers capable of the reverse engineering are in short supply forcing the trend towards greater automation.

Near real time identification of malware is not feasible in many cases leading to some delay whilst protection is instigated and alternative routes established. The case when data is corrupted and not recognised will remain but should be minimised. Decision makers must be cognisant of a potential threat.

SYMPOSIUM

General Impression

The symposium provided a forum to discuss Information Assurance and Cyber Defence topics with presentations supporting a number of good papers reflecting the progress made in the discipline. The quality of the papers was generally good with the content aligned with the call for papers. In some instances a project was addressed from several angles with multiple papers. It was opportune that Mobile Ad hoc Networks received additional time which reflects their vulnerability. The emphasis on reducing the latency through software decision process was evident, justified because a man in the loop would not be able to absorb the vast amount of data necessary. There are a large number of declared incidents where malware has been identified and the number continues to rise demanding prudence on behalf of the users. The proliferation of processors used by the general public attracts third parties to exploit the position whether as an intellectual exercise or for malicious purposes. The move towards cloud computing opens up further avenues The malware can be grouped into categories and a wide spectrum has already been observed with different forms evolving at each generation. Control of processors by bot herder (bot masters) exercising instructions over the net using IRC or HTTP is common place with some hosts unaware of their contribution. This symposium exposed a number of potentially useful techniques to identify intruders and provides a background of references. Information Assurance remains a critical discipline with the emphasis on formal analysis to understand the actions.

The programme was well structured and mirrored the aims within the call for papers. The grouping fell under the titles of:

- Malicious code and APTs (Advanced Persistent Threats)
- Architectures
- MANETs (Mobile Ad hoc Networks) and Sensor Networks
- Cryptography and its Application
- Detection and Reaction
- Selected Technologies

Seven Session chairs were selected from the seventeen members of the technical committee. I commend their actions both in providing the background to the authors and preparing questions of clarification. The technical committee also contained members who were not active during the symposium, I must assume they had assisted to solicit the papers and adjudicate on the selection of abstracts to go forward. Timing of papers and allowing discussion and questions after each paper was appropriate. Coffee breaks allowed further clarification with the authors which was seen to be utilised.

The symposium attracted some 120 scientists with a high level of attendance throughout. The distribution of contributors by country did not reflect the research profile with the contribution aligned to the major players within the technical committee. Whilst this is to be anticipated it is somewhat disappointing, and the technical committee members should be encouraged to obtain abstracts from experts outside their own country. I had the advantage to receive an early distribution of the papers which was beneficial; the delegates had the opportunity to access the papers but with limited time. Provision to increase this available time with the proviso that the paper is subject to revision could be considered with advantage.

The aims expressed in the call for papers are laudable, timely and consistent with the priorities declared by the CTO Board. I understand that the response to the call for papers permitted a degree of filtering. In some areas the symposium would have benefited by including additional topics to bolster the programme; disappointing given the known extensive work in the discipline not constrained by classification. The

selection of presentations from the abstracts submitted cannot be rigorous and it is important to maintain a balance of the disciplines which was achieved, unfortunately considerable redundancy was evident with the keynote speakers which should have been identified when the invitations were issued. In the future, symposium chairman should coordinate the content and declare the boundaries of the presentation as part of the invitation. In this instance the Keynote speakers could have been directed towards a technical appraisal, Authors from academia were conspicuous by their absence; one author had an academic address but delivered a system approach more representative of a government body.

The room was well appointed and gave excellent views of the podium and the screens. Arrangements for discussion in the margins were good particularly during coffee breaks, an essential part of any symposium. Access to the internet was arranged at the location allowing good high speed connectivity during breaks. Network address and passwords were readily available to delegates which also gave access to the papers lodged on the CTO web site.

Analysis of Questionnaires

Regrettably insufficient returns were received to be of any significance. It is disappointing that despite each delegate having a questionnaire in the welcome pack that the response was so poor, (post meeting note: Despite offering the delegates the ability to lodge their response by email only two were completed.) It may be prudent for the chair to remind the delegates just before the close to enable the organisers to react to specific features. The feedback is important to refine the logistics and also to provide third party assessment of the relevance of the topics and the technical content from a delegate's perspective.

Summary of the Papers

Welcome speech and Introduction. BGen Veit gave a warm welcome to Koblenz and identified the opportune time which corresponds with a restructuring within the German procurement process which will give more emphasis of Information Management to operational staff. Dr Vezina as chair of the IST Panel presented the goals of the CTO which are similar to those of the retiring RTO namely: advertise research activity, enable security and support the overall decision process. This was achieved through effective collaboration of some 3000 scientist which will be maintained within the CTO. The mechanisms to success remains active Task Groups, Lecture Series and Symposia, Dr Martini as chair of the symposium opened the technical session with reference to the preceding symposium on this subject initially organised for Turkey. He emphasised the need to exchange ideas to counter intrusion primarily because of the global scale of the potential threat.

Keynote 1: Niggemann A view of Cyberspace from a German perspective with a strong bias towards application. The agency for which the author is Director necessarily has close ties with other agencies and departments, emphasising the need for sharing of observations and impact. The output from his staff is a collection of Best Practice Manuals and Situation Reports. He gave an appraisal of the evolution of the attackers from a non-profit exercise to professional exploitation thence espionage and the logical extension to cyber terrorism. All systems are vulnerable including citizens IT which can readily host botnets. Germany retains a Crisis Reactive Centre which has the ability to generate timely countermeasures. The documents produced are widely available with few regarded as confidential easing collaboration, regarded as essential. Provision is made for sources to remain anonymous when reporting an attack.

Session 1 Malicious Code and APTs

Paper 1 Clone Search for Malicious Code Correlation: Charland This paper reports on the work undertaken in Canada on clone search to reduce the workload on code analysts. Authors of malware follow the practice of reusing code and exchange code within their community. The task is made harder for the legitimate used because of the need for the intruder to hide their efforts. It is important to identify the

malicious code and establish the significance at an early phase. Particularly important if the malware is customised for the specific system under study. The paper describes successful extraction of both syntactic and semantic clones. The latter is more difficult because it is syntactically dissimilar but has the same functionality. The methods have been validated by empirical study but remain in a state of flux with continual evolution on the part of the malware authors. The results presented look encouraging and offset the limited group trained to undertake reverse engineering

Paper 2 Automatic Extraction of Domain Name Generation Algorithms from Current Malware: Barabosch This addresses the issue of bot control. Three architectures have been currently observed a) Centralised b) Decentralised and c) Locomotion. It is necessary to identify the properties of a Dynamic Name Generation Algorithm for which four classes are possible. These are deterministic and non-deterministic each of which can be time dependent or time independent. Cases were shown for detection with some success. Domain name registration by law enforcement agencies would ease the position.

Paper 3 Multi-Agent Anomaly Based APT Detection: Mees The aim is to identify processors hosting malware by observing their behaviour at coke points. Two methods were offered a) looking at the protocol and b) identifying periodic effects in the spectral analysis of http. The issue is to attempt to reduce the number of false positives by invoking fuzzy logic methods within a multi-agent configuration. The aggregation from each agent is combined with weights allocated to the agents' assessment. In answer to a question from the floor it was acknowledged that if the malware mimics human behaviour it will not be identified. The system works on offline log files and data from mail servers and relies on post processing, hence incurs latency.

Session 2 Architecture

Paper 4 Real-Time Automatic Risk Assessment within Protected Core Networking: Haines This paper attracted the best paper award. It is a discussion of the protected core network (PCN) with a view to create an automated risk assessment. A full description of the architecture is available in the paper but in essence the users are part of a cloud and communicate over a black network. Within the PCN enhanced nodes are established to interface with other subsets (PCS). An assessment of the risk is derived for each section and the action taken on inference drawn locally. No section shares the inference. Collaboration is achieved through willing participants without exposing individual attributes. Assessment of risk is made using a Bayesian model which will have associated computational overheads when changes are made. Scalability remains an issue.

P*aper 5 A QoP Framework Supporting CIA Negotiations and Trust-Based Path Selections: Haines* A second paper by Haines addressing Quality of Protection over the same core network (PCN). The project looked at an holistic approach with a description of the parameters. Further work is required to refine the metrics employed. A question was asked wrt Quality of Service cf Quality of Protection which generated some discussion; no conclusive answer was provided.

Paper 6 A Secure NEC Enabled Architecture by Disentangling Infrastructure, Information and Security: Verkoelen. The third paper in this session exposed the related NEC architecture. This will accommodate migration from coalition operations to scenarios which include non NATO participants and eventually NGOs. The proposal is to separate the information boundaries from the infrastructure and reduce the size of the security domain. Information labelling is a pre-requisite with its own trusted operating system. The scheme did not achieve universal approval. A question raised from the floor about the impact of the increase in cryptographic equipment necessary was answered that potentially software methods could be employed.

Paper 7 Tracking Incidents across Translational Boundaries: presented by Mclean A problem was identified when attempting to locate the source of corruption when processors share IP addresses pertinent in large networks with processors tiered. The interface unit possibly a router will hold the information but the overheads preclude storing the data for any length of time. The paper addresses a method whereby

sensors are installed both inboard and outboard of the translation device so as to not impact on its performance. A proof of concept was discussed in which the payload was used as an identifier with an appropriate hash.

Session 3 MANETs and Sensor Networks I

Paper 8 Intrusion Detection in Tactical Mobile Ad Hoc Networks Using Game Theory: presented by Mason The project described modelled the MANET as a dynamic Bayesian game to establish the behaviour when an illicit node is introduced. The paper gives a mathematical thesis which was suppressed in the presentation. Results were provided with different strategies with a conclusion that the users must have a good grasp of the characteristics of the communications link. It was proposed from the floor that the malicious node could report a legitimate node as rouge; a viable situation but not considered in the paper.

Paper 9 was withdrawn without presentation and is not available for review.

Paper 10 A Covert System Monitoring Function for Mobile Ad Hoc Networks: Mason A second paper by Mason aimed at identifying wormholes through diversity of routing protocols. Examples were shown by using OLSR and AODV on the source information. Caution is required to avoid adversely impacting the performance by introducing two probes each using bandwidth. A technique to hide the secondary protocol was thought possible but not described, it will undoubtedly add to the resilience.

Keynote 2: Lefebvre A Canadian perspective of the general situation again identifying an agency who publish manuals to inform and assist users. The strategy adopted is a direct result of discussions with Government, Industry and Academia. No commercial software was identified to resolve the issues observed or model the impact resulting in the need to write ad hoc models. Visualisation was highlighted as a known weakness. The speaker brought the activities of IST-081,IST-108 and IST-109 to the attention of the audience which provide a useful source of further information.

Session 4 Cryptography and its Application

Paper 11 Secure Information Sharing Using Attribute Based Encryption: Cullen An exposé of a relatively new approach to prevent inappropriate transfer of knowledge employing attribute based encryption. The principle is to use a public key to encrypt the data using a comprehensive set of attributes. The users will have a private key with their permitted attributes embedded within the key, thus only decrypting data with those declared attributes. A limited demonstration was presented showing some benefits with a linear relationship in terms of scalability. No evidence of formal analysis was given, thought necessary in this critical domain.

Paper 12 A New Approach of Generating Key Dependent S-Boxes in AES: Stoianov A proposal again without formal analysis to increase the degree of protection afforded by S-Boxes. A set of matrices were tested with the software simulator developed by WP8 in the Project INDECT and showed encouraging results. Some reservations were raised from the floor about the expansion to 256 options; the inclined reader is directed to the paper and associated references.

Paper 13 Secure Authentication Using PIN Based Cancellable Fingerprint Templates: Xiao. The paper offers a method to protect the source information by applying a transform,whereby if the transmitted data is compromised the source is still viable. The author specifically addressed the impact of compromise of fingerprint minutia which define an individual particularly for authentication or key release. In essence the comparison was undertaken in a transform domain, satisfactory if one to one mapping can be assured.

Paper 14 Digital Vaccines: Using Identity Based Digital Signatures for Blue Forces Identification in Cyberspace: Kiviharju An equivalent IFF mechanism was offered to enable friendly nodes to identify themselves in cyberspace. A model based on biological behaviour was postulated with dispersed mechanism

needing multiple agreements. PKI certificates were shown not to be sufficient for this application with the proposal to combine HIBS and SSS based on tagged signatures.

Session 5 Selected Technologies

Paper 15 A Pareto Approach to Software Dependability: Bryant A general paper addressing the system implications from a concept. Comments were made so that developers do not propagate error previously identified. Currently some 800 weaknesses are published one in particular associated with buffer overflow dates back to early development in the sixties. The author made the observation that progress can be made by implementing small changes to achieve trustworthy software and encouraged designers to tackle the declared weaknesses.

Paper 16 A survey in Threat Detection: Jasiul A paper reporting on the progress of INSIGMA providing pointers to trends in detecting anomalies. The inclined reader is directed to not only the paper presented at the symposium but also exposure of the findings in earlier symposia.

Paper 17 The Multicast Internet Key Exchange (MIKE) in Tactical Ad Hoc Networks: Hegland Addressed the problem associated with members joining a net. MIKE was offered as a potential solution using key trees to assist organisation. It was recognised that MIKE is not fully mature and needs further work but shows potential. A question was raised about split and rejoin, the reply was that members would retain the key on split whilst rejoining would need to reinitialise if the key held was no longer used by the parent net.

Session 6 Detection and Reaction

Paper 18 Proactive Detection and Automated Exchange of Network Security Incidents: Kijewski . A comparison was made between Reactive and Proactive detection methods, it was stated that a lot of incidents go unreported. A useful matrix comparing properties of the various methods considered was presented. In answer to a question from the floor the author indicated that the tools were unable to predict threats.

Paper 19 Detection of Multistage Attack in Federation of Systems Environment: Berezinski. Provided a description of a prototype model designed under project SOPAS. The aim is to prevent damage caused by malware which could be inadvertently hosted. The processor infected could be internal to the system or ingress through an internet gateway. The scheme employs Snort and other open source software to detect anomalous behaviour which could itself allow back door installation of malware. It is proposed to use Petri nets in future forensic analysis.

Paper 20 Automatic Reaction to Cyber Attacks on the Basis of Remote Secure Controller: Sliwa. Paper 20 is a second paper on SOPAS. Emphasis in this paper is directed at the Decision Module developing predominantly automatic responses governed by declared rules but assisted by a human in the loop. The man also acts as administrator reacting to information presented on a graphical interface. A test bed has been built to assess the reaction time which for RCS was some 900 msec compared with Bind9 of some 1200 msec which included a 300 msec reset.

Paper 21 was withdrawn and will not be published.

MANETs and Sensor Networks II

Paper 22 Supporting Network-Wide Situational Awareness in Tactical MANETs by Local Observations: Hunke. This paper concentrated on networks in which sensors are generally limited by available power forcing passive monitoring. Inference was established by combining local observations. Some encouraging experimental results were presented with further work identified to incorporate a higher degree of sophistication in the topology. The work is closely coupled to projects MITE and RITA. A question was posed relating to the performance in radio silence which by definition for passive systems becomes an issue.

Paper 23 Lightweight User Authentication in Wireless Sensor Networks: Mason. Exposed a modification to improve security portals. The performance was enhanced by incorporating mutual authentication endorsed by formal analysis.

CONCLUSIONS

The symposium achieved the objectives of exposing the general performance of selected projects and provided a raft of references, greater emphasis on formal analysis would have enhanced the proceedings. The technical content was satisfactory but with room for improvement. A number of papers passed peer review we should strive for a full complement. It remains essential in a research environment to attract high quality papers and presentations to explore aspect from prompts given during the discussions. The forum allows interaction between military advisers and scientists; it would be of further advantage if academics could voice their research and have an appreciation of the operational issues.

It is recommended:

- that the technical committee is selected from knowledgeable engineers who can devote appropriate time to the activity;
- that greater emphasis is afforded to obtain feedback through the questionnaire.

The symposium was timely and exposed some appropriate work. I commend the technical committee for their good work.