Information Assurance and Cyber Defence

(RTO-MP-IST-091)

Executive Summary

Information Assurance and Cyber Defence represent a broad domain, this Symposium addresses some of the research topics in this field which are regarded as important; not only scientifically, but also operationally and politically. Progress is reported in the disciplines of:

- Intrusion Detection, Protection and Countermeasures;
- Security Models and Architectures;
- Security Policies, Evaluation, Authorisation and Access Control; and
- Network and Information Security Awareness.

Various projects, both national and with international collaboration, are discussed in the proceedings of the Symposium. Progress described is significant with some mechanisms able to detect abnormal behaviour confirmed through experimentation. Of interest is the detection of bots; current methods achieving some success by applying Genetic Algorithms, it is hoped that detection will be more readily achieved in the near future. Transfer of information about a potential threat particularly across national boundaries eases the situation and brings together a diversity of surveillance techniques. Establishing mutual trust is paramount to achieve a timely reaction with schema described to improve confidence. The installation of dedicated CERT (Computer Emergency Response Teams) has shown merit in Poland and should be considered elsewhere. A potential solution to ease security by employing the necessary and sufficient core of open systems enhanced by weaving in additional security features is advocated and looks encouraging. A main threat to systems remains the disillusioned system operator who is able to bypass a number of the security features.

Several papers address the PCN (Protected Core Network) concept which appears to be viable. An exercise/ experiment was conducted in the Baltic which was successful in showing the principles and is reported in the proceedings. A warning about RFIDs and simple wireless devices is included describing the vulnerability of systems to replication of bugs which will corrupt the data and allow attackers to set up false nodes.

A proactive stance to predict the next generation of threats is advocated and use of Genetic Algorithms thought appropriate. The mathematics of this discipline are sufficiently advanced that some confidence is generated in the predictions and several groups have the expertise to select the evolutionary process.

The heavy reliance on software in both military and civilian systems leaves the users vulnerable to cyber attack. Whilst the defender has the benefit of knowing his system the attacker has leverage in that a small resource can cause major disruption and hence vigilance by all users is required. The proceedings include papers by the invited speakers addressing observations of attacks and good practice to limit the impact of such attacks. The Symposium proceedings provide a considered assessment of the subject and identify areas where further research would be beneficial.

Assurance de l'information et cyberdéfense

(RTO-MP-IST-091)

Synthèse

L'assurance de l'information et la cyberdéfense représentent un vaste domaine, et ce symposium aborde certains thèmes de recherche de ce domaine considérés comme thèmes majeurs ; non seulement d'un point de vue scientifique, mais également d'un point de vue opérationnel et politique. On note des progrès dans les disciplines suivantes :

- Détection d'intrusion, protection et contre-mesures ;
- Modèles et architectures de sécurité ;
- Politiques de sécurité, évaluation, agrément et contrôle d'accès ; et
- Sensibilisation à la sécurité du réseau et de l'information.

Plusieurs projets d'envergure nationale et internationale sont traités dans les actes du symposium. Les progrès décrits sont significatifs, avec des mécanismes capables de détecter un comportement anormal confirmé grâce à l'expérimentation. La détection de « bots » est particulièrement intéressante ; les méthodes actuelles ayant obtenu certains résultats grâce à l'application d'algorithmes génétiques, nous espérons que la détection atteindra un niveau de maturité technologique plus élevé dans un futur proche. Le transfert d'informations concernant une menace potentielle, par-delà les frontières nationales, facilite la situation et rassemble diverses techniques de surveillance. L'établissement d'une confiance mutuelle est crucial pour obtenir une réaction rapide selon le schéma décrit et visant à améliorer la confiance. L'installation de CERT dédiées (Equipes d'intervention en cas d'urgence informatique) a prouvé leur utilité en Pologne et doit être envisagée ailleurs dans le monde. Une solution potentielle est préconisée et paraît encourageante : elle consiste à faciliter la sécurité grâce à une utilisation fondamentale et suffisante du cœur des systèmes ouverts, améliorés par le maillage de dispositifs de sécurité additionnels. La principale menace envers les systèmes demeure l'opérateur système déçu et capable de contourner un certain nombre de dispositifs de sécurité.

Plusieurs articles traitent du concept du RCP (Réseau central protégé) qui apparaît comme une option viable. L'exercice/expérience menée en mer Baltique en a démontré les principes avec succès et est décrite dans les actes du symposium. Un message d'avertissement concernant l'identification par radio-fréquence (RFID) et les dispositifs simples sans fil est inclus au travers d'une description de la vulnérabilité des systèmes face à la réplication des bogues qui corrompent les données et permettent aux agresseurs de mettre en place de faux nœuds.

Il est recommandé d'adopter une approche proactive visant à prévoir la prochaine génération de menaces, et l'utilisation d'algorithmes génétiques est jugée appropriée. Les mathématiques de cette discipline sont à un niveau suffisamment avancé pour générer une certaine confiance dans les prévisions et plusieurs groupes possèdent l'expertise requise pour sélectionner un processus évolutif.

La grande dépendance à l'égard des logiciels dans les systèmes civils et militaires rend les utilisateurs vulnérables aux cyberattaques. Tandis que le défenseur a l'avantage de connaître son système, l'agresseur possède la force, car une toute petite ressource peut être à l'origine de perturbations majeures, et il est par conséquent important que tous les utilisateurs fassent preuve de vigilance. Les actes comprennent des articles écrits par les intervenants invités décrivant les observations d'attaques et les bonnes pratiques à respecter pour limiter l'impact de telles agressions. Les actes du symposium fournissent une évaluation minutieuse du sujet et identifient les domaines où des recherches approfondies s'avèreraient utiles.