Information Assurance and Cyber Defence

(STO-MP-IST-111)

Executive Summary

Information Assurance and Cyber Defence is a critical aspect of not only Military Operations but also has a significant impact on the civilian population. A large number of attacks have been identified and are evolving; as one counter is developed the next generation of threat is observed. The NATO Science and Technology Organisation has sponsored a number of activities for which this symposium was a means of disseminating the research activities in this discipline by the contributing Nations. The papers address six topic areas: Malicious code and Advanced Persistent Threats (APT), Architecture, MANETs, Cryptography, Detection and Reaction and Selected Technologies.

The papers on malicious code show developments in analysing code to identify clones giving an ability to automate some aspects of the labour intensive activity. Other papers provide a raft of references and a matrix to compare the various detection methods. Advanced Persistent Threats, by definition, attempt to obfuscate the code to allow back door entry without the host being aware. Several detection approaches were reported with some success. Sensing the behaviour and the handling of address generators within the malicious code are examples. The military in general and NATO task groups including IST-069 advocate Protected Core Networking which was discussed and the papers provide extensive references. Several aspects to protect MANETs were raised primarily to use cryptographic methods to maintain assurance that the data transferred is reliable and from a legitimate source. Joining and leaving the network are of particular concern; methods to probe the net to establish trusted users are presented. Probing has an overhead particularly when diversity of techniques is deemed necessary, caution was advised to ensure that the appropriate balance is achieved. A secure channel which has zero bandwidth available for the transport of information is of little value. Alternative assurance by using encryption on the data or attributes may be worthy of consideration but care should be exercised to ensure that when applied to a particular scenario a formal analysis meets aspirations.

A large number of issues have been presented; the inclined reader can use the proceedings and the associated references as a good basis for further research. The move towards cloud computing raises challenges to maintain assurance, some mitigating methods are offered in the proceedings. Counters to malicious code demand analysis and will incur latency between detection and protection. An ideal would be to have a high degree of automation with some element of prediction. The users must be aware of the situation and employ techniques to establish as much assurance in the network and the information transferred as possible whilst ensuring currency of protective techniques.

Sûreté de l'information et cyber défense

(STO-MP-IST-111)

Synthèse

La sûreté de l'information et la cyber défense sont non seulement deux aspects critiques des opérations militaires, mais ont également un impact important sur la population civile. Un grand nombre d'attaques ont été identifiées et évoluent ; lorsqu'une contre-mesure est élaborée, la génération suivante de menaces apparaît. L'Organisation pour la science et la technologie de l'OTAN a parrainé plusieurs activités pour lesquelles ce colloque était un moyen de faire connaître les activités de recherches nationales dans cette discipline. Les articles présentés traitent de six domaines : le code malveillant et les menaces persistantes avancées (APT), l'architecture, les MANET, la cryptographie, la détection et la réaction et les technologies sélectionnées.

Les articles sur le code malveillant montrent l'évolution dans l'analyse du code afin d'identifier les clones, ce qui permet d'automatiser certains aspects de cette activité à forte contrainte de main-d'œuvre. D'autres articles fournissent beaucoup de références et une matrice pour comparer les diverses méthodes de détection. Les menaces persistantes avancées tentent, par définition, d'obscurcir le code pour permettre l'entrée par des moyens détournés sans que le système hôte s'en aperçoive. Plusieurs approches de détection assez efficaces ont été présentées, notamment la détection du comportement et le traitement des générateurs d'adresse au sein du code malveillant. Les militaires en général et les groupes de travail de l'OTAN, dont l'IST-069, sont les partisans d'un réseau central protégé, qui a été examiné, et pour lesquels les articles présentés fournissent des références complètes. Plusieurs aspects ont été soulevés au sujet de la protection des MANET, principalement l'utilisation de méthodes cryptographiques pour maintenir l'assurance que les données transférées sont fiables et proviennent d'une source légitime. Les opérations de connexion et déconnexion du réseau sont particulièrement préoccupantes ; des méthodes de sondage du réseau validant les utilisateurs de confiance sont présentées. Le sondage a un coût, particulièrement lorsque la diversité des techniques est jugée nécessaire. Il a été conseillé de faire preuve de prudence pour s'assurer que l'équilibre approprié soit atteint. Une voie sécurisée dont la bande passante est indisponible pour le transport d'information a peu de valeur. Il peut valoir la peine de considérer une autre possibilité, à savoir le chiffrement des données ou attributs, mais il faut alors veiller à ce qu'une analyse formelle réponde aux attentes lorsqu'elle est appliquée à un scénario en particulier.

Un grand nombre de questions ont été avancées. Le lecteur intéressé peut se reporter aux actes et à la bibliographie associée pour en savoir plus. Le passage au cloud computing soulève des problèmes de préservation de la sûreté ; les actes proposent quelques méthodes. Les contre-mesures au code malveillant nécessitent de l'analyse et entraîneront un temps d'attente entre la détection et la protection. L'idéal serait de disposer d'un degré élevé d'automatisation avec quelques éléments de prédiction. Les utilisateurs doivent connaître la situation et employer des techniques qui créent autant de sûreté que possible pour le réseau et les informations transférées, tout en permettant aux techniques de protection de devenir courantes.