NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

AC/323(IST-041)TP/27

www.rta.nato.int

RTO MEETING PROCEEDINGS **MP-IST-041**

Adaptive Defence in Unclassified Networks

(La défense adaptative pour les réseaux non classifiés)

Papers presented at the RTO Information Systems Technology Panel (IST) Symposium held in Toulouse, France, 19-20 April 2004.

Published November 2004

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

AC/323(IST-041)TP/27

www.rta.nato.int

RTO MEETING PROCEEDINGS **MP-IST-041**

Adaptive Defence in Unclassified Networks

(La défense adaptative pour les réseaux non classifiés)

Papers presented at the RTO Information Systems Technology Panel (IST) Symposium held in Toulouse, France, 19-20 April 2004.

The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote co-operative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective co-ordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also co-ordinates RTO's co-operation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of co-operation.

The total spectrum of R&T activities is covered by the following 7 bodies:

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS Studies, Analysis and Simulation Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier co-operation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

Published November 2004

ISBN 92-837-0039-2

Adaptive Defence in Unclassified Networks

(RTO-MP-IST-041)

Executive Summary

Classified military networks are designed to maintain functionality under active attack. Their robustness comes from careful design, controlled isolation and purposely limiting functionality. Unclassified networked systems represent the vast majority of military information system and are very important for NATO by providing services such as email, logistics support, unclassified file transport, and access to the vast amount of information on the World Wide Web. Similarly, governments and the military operate web sites and other services that are of critical importance to the civil community, particularly in times of crisis. For military and government users ready access to external services can be pivotal to maintenance of efficient operations. Techniques employed to protect classified information systems for many applications are too limiting and costly to apply to unclassified applications where the benefits of reasonably open access greatly outweigh the potential risks. However, such systems still need protection, but not from loss of information so much as from denial of service and the potential for corruption of information. Balancing protection and capability is a complex problem. The goal of dynamically balancing access while limiting real damage is in many respects a more complex problem than absolute protection of more limited core services. This symposium addressed NATO interests and issues in operating unclassified computing systems and networks while maintaining desired levels of assurance.

The symposium provided an interdisciplinary forum for research scientists, military experts, and system engineers to present the state of the art of research and technology in the protection of unclassified computer systems and networks. The broad scope of topics was discussed by an excellent keynote speech and 21 interesting and well appreciated papers which were presented in 7 technical sessions to an audience of approximately 100 participants. The symposium opened with a keynote address by Professor Richard Kemmerer of the University of California. His address, entitled “Designing a Web of Highly Configurable Intrusion Sensors”, described a framework for the development of intrusion detection systems that overcomes the limitations of more traditional approaches that are often developed in an ad hoc manner for certain types of domains and are hard to configure, extend, and control remotely. This theme was carried over into a session on Intrusion Detection and Response that looked at issues of developing cooperative intrusion detection components in dynamic coalition environments, intrusion tolerance, and reactions. A paper from this session on selecting appropriate countermeasures was awarded the “Best Paper Award”.

A session on Coalition Networks looked at various methods for securing unclassified coalition networks, including software-engineering based approaches, Virtual LANs, and the application of Virtual Machines. Other sessions focused on specific aspects of this problem. For example, a session on Honeypots looked at the use of honeypot technology to gather information about attack processes that can be found on the Internet and at ways that honeypot systems can emulate database servers, and a session on Servers and Viruses looked at improved ways for deploying antivirus technology, ways to protect public servers, and the effects of outsourcing government web sites. A session on Network Technology looked at issues of vulnerability assessment, passive network discovery, and network monitoring, while a session on securing networks looked at ways to use commercial messaging software securely, ways to enforce security policies in heterogeneous environments, technology to use public networks without being subject to traffic analysis, and ways to enforce security policies on secure socket layer connections. A final session addressed the problem of safely using COTS by breaking up system monocultures and by building trusted paths within COTS components.

La défense adaptative pour les réseaux non classifiés

(RTO-MP-IST-041)

Synthèse

Les réseaux militaires classifiés sont conçus de façon à conserver leur intégrité opérationnelle, même en cas d'attaque directe. Leur robustesse est le résultat d'une conception soignée, d'une isolation contrôlée et d'un nombre limité de fonctionnalités. Les systèmes en réseaux non classifiés représentent la grande majorité des systèmes d'information militaires et sont très importants pour l'OTAN, puisqu'ils fournissent des services tels que le courrier électronique, le soutien logistique, la transmission de fichiers non classifiés et l'accès à l'énorme quantité d'informations disponibles sur la toile mondiale. De la même façon, les gouvernements et les militaires exploitent des sites Web ainsi que d'autres services qui sont d'une importance vitale pour les civils, en particulier en temps de crise. Pour ces utilisateurs, l'accès direct à des services externes peut-être déterminant pour le maintien d'opérations efficaces. Pour bon nombre d'applications non classifiées, les techniques utilisées en vue de la protection des systèmes d'information classifiés sont trop contraignantes et trop coûteuses, car, dans ces cas, les avantages que comporte un accès relativement libre l'emportent largement sur les risques éventuels. Cependant, ces systèmes ont encore besoin de protection, non pas contre la perte d'informations, mais plutôt contre le refus de services et la possibilité d'altération des données. Concilier protection et capacité est un problème complexe. A bien des égards, l'objectif qui consiste à concilier ces éléments de façon dynamique, tout en limitant les dommages réels, est un problème plus complexe que celui de la protection intégrale de certains services essentiels plus restreints. Ce symposium a fait le point sur les intérêts de l'OTAN, ainsi que sur les problèmes qu'elle rencontre pour assurer l'exploitation de systèmes et de réseaux informatiques non classifiés dans des conditions de sécurité acceptables.

Ce symposium a servi de forum interdisciplinaire, permettant aux chercheurs scientifiques, aux spécialistes militaires, et aux ingénieurs systèmes de présenter l'état actuel de la recherche et de la technologie dans le domaine de la protection des systèmes et des réseaux informatiques non classifiés. L'ensemble des sujets a été abordé dans un excellent discours d'ouverture, ainsi que dans 21 communications intéressantes et bien accueillies, présentées au cours de 7 sessions techniques devant une assistance d'une centaine de participants. Le symposium a débuté par un discours d'ouverture prononcé par le Professeur Kemmerer, de l'Université de Californie. Dans sa présentation, « La conception d'un réseau de capteurs d'intrus facilement configurable », il a fourni la description d'un cadre pour le développement de systèmes de détection d'intrus qui s'affranchit des limitations imposées par les systèmes plus classiques qui sont souvent développés pour la circonstance au profit de certains types de domaines et qui sont difficiles à configurer, à améliorer et à télécommander. Ce thème a été poursuivi lors d'une session sur la détection et la réponse aux intrus, couvrant le développement en coopération de dispositifs de détection d'intrus en environnement dynamique de coalition, la tolérance aux intrus et les réactions. L'une des présentations de cette session a été désignée « meilleure communication du symposium ».

La session sur les réseaux de coalition a permis d'examiner différentes méthodes de sécurisation des réseaux de coalition non classifiés, y compris des approches basées sur le génie logiciel, les LAN virtuels et la mise en œuvre de machines virtuelles. D'autres sessions ont privilégié des aspects spécifiques de ce problème. Par exemple, une session sur les technologies de pointe a examiné leur capacité de rassembler des informations sur les mécanismes d'attaque affichés sur l'Internet, ainsi que leurs possibilités d'émulation de serveurs de bases de données. Une autre session sur les serveurs et les virus a examiné les nouvelles applications des technologies antivirus, la protection des serveurs grand public et les conséquences de la sous-traitance des sites web gouvernementaux. Une session sur les technologies des réseaux a permis d'étudier des questions concernant l'évaluation de la vulnérabilité, la découverte des réseaux passifs, et le contrôle des réseaux. Une autre session, sur la sécurisation des réseaux, a examiné la sécurisation des logiciels de messagerie du commerce, la mise en application de politiques de sécurité en environnement hétérogène, les technologies permettant d'exploiter les réseaux publics sans être soumis aux analyses de trafic et la mise en application de politiques de sécurité concernant les connexions sécurisées au niveau de la couche « socket ». La session finale a examiné une approche du problème de la mise en œuvre de systèmes COTS en toute sécurité, qui consiste à décomposer les monocultures inhérentes aux systèmes pour ensuite créer des chemins fiables au sein des composants COTS.

Table of Contents

SESSION III – HONEYPOTS
Chairman: Dr. G. EIZENBERG, FR

SESSION IV – SERVERS AND VIRUSES
Chairman: Mr. P. CHAUVE, FR

SESSION V – NETWORK TECHNOLOGY
Chairman: Dr. J. LEFEBVRE, CA

SESSION VI – SECURING NETWORKS
Chairman: Mr. G. HALLINGSTAD, NO

SESSION VII – DEALING WITH COTS
Chairman: Dr. R. SHUMAKER, US

Information Systems Technology Panel

ACKNOWLEDGEMENTS/REMERCIEMENTS

The IST Panel wishes to express its thanks to the French RTB members to RTA for the invitation to hold this Symposium in Toulouse and for the facilities and personnel which made the Symposium possible.

Le Panel IST tient à remercier les membres français du RTB auprès de la RTA de leur invitation à tenir cette réunion à Toulouse, ainsi que pour les installations et le personnel mis à sa disposition.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	RTO-MP-IST-041 AC/323(IST-041)TP/27	ISBN 92-837-0039-2	UNCLASSIFIED/ UNLIMITED

5. Originator

Research and Technology Organisation
North Atlantic Treaty Organisation
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Adaptive Defence in Unclassified Networks

7. Presented at/Sponsored by

The RTO Information Systems Technology Panel (IST) Symposium held in Toulouse, France, 19-20 April 2004.

8. Author(s)/Editor(s)	9. Date
Multiple	November 2004
10. Author's/Editor's Address	**11. Pages**
Multiple	288 (text) 497 (slides)

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other RTO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Communications networks
Computer information security
Computer networks
Computer security
Denial of service attacks
Design
Electronic security
IDS (Intrusion Detection Systems)
Information assurance
Information security
Information systems
Integrated systems
International cooperation
Intrusion detectors
Secure communication
Surveillance
Systems engineering
Threat evaluation
Vulnerability

14. Abstract

This volume contains 21 papers, presented at the Symposium of the Information Systems Technology Panel (IST) held in Toulouse, France, from 19th to 20th April 2004.

The papers were presented in seven sessions covering the following headings: Coalition Networks; Intrusion Detection and Response; Honeypots; Servers and Viruses, Network Technology; Securing Networks; Dealing with COTS.

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DIFFUSION DES PUBLICATIONS

RTO NON CLASSIFIEES

Les publications de l'AGARD et de la RTO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la RTO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la RTO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (www.rta.nato.int) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der
Bundeswehr (FIZBw)
Friedrich-Ebert-Allee 34, D-53113 Bonn

BELGIQUE
Etat-Major de la Défense
Département d'Etat-Major Stratégie
ACOS-STRAT – Coord. RTO
Quartier Reine Elisabeth
Rue d'Evère, B-1140 Bruxelles

CANADA
DSIGRD2
Bibliothécaire des ressources du savoir
R et D pour la défense Canada
Ministère de la Défense nationale
305, rue Rideau, 9e étage
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Defence Research Establishment
Ryvangs Allé 1, P.O. Box 2715
DK-2100 Copenhagen Ø

ESPAGNE
SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

ETATS-UNIS
NASA Center for AeroSpace
Information (CASI)
Parkway Center, 7121 Standard Drive
Hanover, MD 21076-1320

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research
General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
H-1525 Budapest P O Box 26

ISLANDE
Director of Aviation
c/o Flugrad
Reykjavik

ITALIE
Centro di Documentazione
Tecnico-Scientifica della Difesa
Via XX Settembre 123
00187 Roma

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Armament Policy Department
218 Niepodleglosci Av.
00-911 Warsaw

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

ROYAUME-UNI
Dstl Knowledge Services
Information Centre, Building 247
Dstl Porton Down
Salisbury
Wiltshire SP4 0JQ

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

NASA Center for AeroSpace Information (CASI)
Parkway Center, 7121 Standard Drive
Hanover, MD 21076-1320
ETATS-UNIS

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council
Acquisitions, Montreal Road, Building M-55
Ottawa K1A 0S2, CANADA

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications RTO et AGARD figurent dans les journaux suivants :

Scientific and Technical Aerospace Reports (STAR)
STAR peut être consulté en ligne au localisateur de ressources uniformes (URL) suivant:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR est édité par CASI dans le cadre du programme NASA d'information scientifique et technique (STI)
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
ETATS-UNIS

Government Reports Announcements & Index (GRA&I)
publié par le National Technical Information Service
Springfield
Virginia 2216
ETATS-UNIS
(accessible également en mode interactif dans la base de données bibliographiques en ligne du NTIS, et sur CD-ROM)

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DISTRIBUTION OF UNCLASSIFIED RTO PUBLICATIONS

AGARD & RTO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all RTO reports, or just those relating to one or more specific RTO Panels, they may be willing to include you (or your Organisation) in their distribution.

RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of RTO reports as they are published, please visit our website (www.rta.nato.int) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Etat-Major de la Défense
Département d'Etat-Major Stratégie
ACOS-STRAT – Coord. RTO
Quartier Reine Elisabeth
Rue d'Evère
B-1140 Bruxelles

CANADA
DRDKIM2
Knowledge Resources Librarian
Defence R&D Canada
Department of National Defence
305 Rideau Street
9th Floor
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

DENMARK
Danish Defence Research Establishment
Ryvangs Allé 1
P.O. Box 2715
DK-2100 Copenhagen Ø

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Friedrich-Ebert-Allee 34
D-53113 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
H-1525 Budapest P O Box 26

ICELAND
Director of Aviation
c/o Flugrad, Reykjavik

ITALY
Centro di Documentazione Tecnico-Scientifica della Difesa
Via XX Settembre 123
00187 Roma

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

POLAND
Armament Policy Department
218 Niepodleglosci Av.
00-911 Warsaw

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

SPAIN
SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Knowledge Services
Information Centre, Building 247
Dstl Porton Down
Salisbury, Wiltshire SP4 0JQ

UNITED STATES
NASA Center for AeroSpace Information (CASI)
Parkway Center, 7121 Standard Drive
Hanover, MD 21076-1320

SALES AGENCIES

NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320
UNITED STATES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council
Acquisitions
Montreal Road, Building M-55
Ottawa K1A 0S2, CANADA

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of RTO and AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
STAR is available on-line at the following uniform resource locator:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR is published by CASI for the NASA Scientific and Technical Information (STI) Program
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
UNITED STATES

Government Reports Announcements & Index (GRA&I)
published by the National Technical Information Service
Springfield
Virginia 2216
UNITED STATES
(also available online in the NTIS Bibliographic Database or on CD-ROM)

ISBN 92-837-0039-2