NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

SYMPOSIUM

INFORMATION ASSURANCE AND CYBER DEFENCE

Sécurité de l'Information et Cyber Défence

IST-091/ RSY-021

organised by the

Information Systems and Technology Panel

to be held in

TEKIROVA,Antalya, Turkey

Monday 26 April 2010 - Tuesday 27 April 2010

This Symposium is open to citizens from NATO, Partner for Peace Nations and Med Dialogue Nations

Latest Enrolment Dates

NATO Nations	**Friday, 16 April 2010**
PfP & Med Dialogue Nations	**Friday, 2 April 2010**

Enrol Online at:

http://www.rto.nato.int

Once your enrolment is validated, you will receive a General Information Package (GIP) giving you further necessary details about the meeting.

If you are unable to enrol via the internet, please contact the IST Panel Assistant at: apaydina@rta.nato.int

All presentations and discussions will be held in either English or French, the official NATO languages. Simultaneous interpretation between the two languages will be provided.

Background

The mission of RTO is to conduct and promote co-operative research and information exchange. RTO consists of a three level organisation: the Research and Technology Board (RTB), the Panels and the Technical Teams. Information Systems Technology Panel (IST) is one of the seven Panels under the RTB and whose role it is to implement, on behalf of the R&T Board, the RTO Mission with respect to Information Systems Technology. The advancement and exchange of techniques and technologies to provide timely, affordable, dependable, secure and relevant information to war fighters, planners and strategists, as well as enabling technologies for modelling, simulation, and training are the focus of this Panel. The Information Systems Technology Panel covers the fields of Information Warfare and Assurance, Information and Knowledge Management, Communications and Networks and Architecture and Enabling Technologies.

Theme

The broad use of information and communication technology in information warfare makes NATO's critical IT infrastructure its most valuable asset and its most vulnerable point of attack. Military platforms are becoming more computer intensive, which means that software is becoming more complex and taking on larger and more important roles, and information systems are being increasingly interconnected, which means that vulnerability in a single program can put an entire infrastructure at risk. As a consequence, information systems security and defence against cyber attacks are major issues and major concerns, especially in joint/coalition operations. Finding effective ways to protect and defend information and information systems by ensuring their availability, integrity, and confidentiality is challenging even with the most advanced technology and trained professionals.

Hence the theme of the symposium is effective ways of defence against cyber attacks and the aim of the symposium is to provide a forum for the scientific and research community to the exchange of state-of-the-art knowledge related to information warfare assurance and cyber defence.

SYMPOSIUM TOPICS

IT systems in today's military assets and C4ISR systems collect, store, evaluate and interpret a massive amount of complex and critical data and information. Hence, these data and information are very vulnerable to attacks, and defence against them is a critical issue that will be focused in this symposium.

Within the theme and this context, topics of interest include, but are not limited to:

- Authentication and Identity Management
- Authorization and Access Control
- Computer Forensics
- Cryptographic Protocols
- Data Integrity and Privacy
- Distributed System Security

- Cryptographic Protocols
- Data Integrity and Privacy
- Distributed System Security

- Information Warfare and Cyber-terrorism
- Information Security Awareness
- Insider Attack Countermeasures
- Intrusion Detection, Prediction and Countermeasures
- Key Management and Recovery
- Military Case Studies, Best Practices and Lessons Learnt
- Network Security
- Policy Issues in Information Assurance
- Secure Collaboration and Information Sharing in Coalition Settings
- Secure Hardware, Biometrics and Smartcards
- Secure Software Technologies
- Security and Assurance for Military Information Systems
- Security Management and Strategy
- Security Models and Architectures
- Security Verification, Evaluations and Measurements
- Survivability and Resilient Systems
- Tactics of Information Warfare: Defence & Attack
- Trust Negotiation, Establishment and Management
- Wireless, Mobile and Sensor Network Security

Programme Committee

Programme Chair

Prof. Nazife BAYKAL
Middle East Technical University, Head of Informatics Dept.
Ankara,Turkey
E-mail: baykal@ii.metu.edu.tr

Members

Dr. Maxwell DONDO
Defense R&D Canada-Ottawa
Canada
Tel: +1 (613) 998 2073
E-mail: maxwell.dondo@drdc-rddc.gc.ca
Dr. Alfred MOELLER
DALO, Applied Reseach Section
Denmark
Tel: +45 (7257) 1550
E-mail: avm@mil.dk
Mr. Régis DUMOND
DGA/D4S/SRTS/OPE
France
Tel: +33 (0) 1 46 19 64 72
E-mail: regis.dumond@dga.defense.gouv.tr

Mr. Gilbert MULTEDO
THALES Communications, SAS/SEA
France
Tel: +33 (1) 41 30 25 02
E-mail: gilbert.multedo@fr.thalesgroup.com
Mr. Olivier de PEUFEILHOUX
EADS/Defence & Communication Systems
France
Tel: +33 (1) 34 63 78 00
E-mail: olivier.de-peufeilhoux@eads.com
Dr. Michael WUNDER
Fraunhofer FKIE
Germany
Tel: +49 (228) 943 55 11
E-mail: michael.wunder@fkie.fraunhofer.de
Dr. Maarten P. I. MANDERS
TNO
The Netherlands
Tel: +31 (70) 374 00 11
E-mail: maarten.manders@tno.nl
Prof. Torleiv MASENG
Norwegian Defence Research Establishment (FFI)
Norway
Tel: +47 (63) 80 72 04
E-mail: torleiv.maseng@ffi.no
Prof. Marek AMANOWICZ
Military Communications Institute
Poland
Tel: +48 (22) 688 55 11
E-mail: m.amanowicz@wil.waw.pl
Mr. Geir HALLINGSTAD
NC3A
The Netherlands
Tel: +31 70 374 37 42
E-mail: geir.hallingstad@nc3a.nato.int
Prof. Bob MADAHAR
DSTL, Information Department
United Kingdom
Tel: +44 (2392) 21 7369
E-mail: bkmadahar@dstl.gov.uk
Dr. John MCLEAN
Naval Research Laboratory, Superintendant, Information
Technology Division
United States
Tel: +1 (202) 767 29 03
E-mail: John.McLean@nrl.navy.mil

RTA Panel Office - Point of Contact

Maj. Vincent MAESTRI
IST Panel Executive
Tel: +33 (0)1 55 61 22 80
E-M: maestriv@rta.nato.int

Mrs Ayşegül APAYDIN
IST Panel Assistant
Tel: +33 (0)1 55 61 22 82
E-mail: apaydina@rta.nato.int

IST-091 Symposium on "Information Assurance and Cyber Defence"

Programme

Monday 26 April 2010

08:00		Registration
08:30		Opening Ceremony: Introduction Prof. Jürgen GROSCHE, IST Panel Chairman, DEU Prof. Nazife BAYKAL, Symposium Chairperson, TUR
09:00		KEYNOTE SPEECH: by Prof. Richard A. KEMMERER, University of California, Santa Barbara, USA
09:30		BREAK

SESSION 1 - Network Security

09:50	**1**	Metrics-based Computer Network Defence Decision Support by L. BEAUDOIN, R. SAWILLA, Defence R&D Canada-Ottawa, CAN
10:15	**2**	Security Shift in Future Network Architectures by T. HARTOG, C. VERKOELEN, H. SCHOTANUS, TNO Information & Communication Technology, NLD
10:40	**3**	FIoVis: Leveraging Visualization to Protect Sensitive Network Infrastructure by J. McHUGH, University of North Carolina and RedJack, LLC, J. GLANFIELD, Dalhousie University, CAN, D. PATERSON, C. SMITH, T. TAYLOR, S. BROOKS, C. GATES, CA Labs. New York, USA
11:00		BREAK
11:30	**4**	Guilt by Associated Based Discovery of Botnet Footprints by A. CAGLAYAN, M. TOOTHAKER, D. DRAPEAU, D. BURKE, G. EATON, Milcord LLC, USA

SESSION 2 - Military Case Studies, Best Practices and Lessons Learned

11:55	**5**	Web Service Security in an Air C2 System by M. UYSAL, J-P. MASSART, NC3A, NLD
12:20	**6**	Strategic Road Map of Network Enabled Capability for Defence in Turkey by M. ARSLAN, SSM, TUR
12:40		LUNCH

POSTER SESSION: Introduction of Posters exhibited during the two days of the Symposium

13:45	**P-01**	Cyber Defence in the Armed Forces of the Czech Republic by J. KADERKA, M. JIRSA, University of Defence, Brno, CZE
	P-02	From Signature-Based Towards Behaviour-Based Anomaly Detection by P. MINARK, J. VYKOPAL, Masaryk University, CZE
	P-03	Coalition Network Defence Common Operational Picture by J. TÖLLE, Fraunhofer FKIE, DEU, L. BEAUDOUIN, M. GRÉGOIRE, DRDC, CAN, R. HALL, Northrop Grumman, USA, C. HEATON, US Air Force Research Laboratory, USA, B. HEINBOCKEL, MITRE, USA, P. LAGADEC, NC3A, J. LEFEBVRE, DRDC, CAN, E. LUIIJF, TNO, NLD, R. McQUAID, MITRE, USA
	P-04	RFID as a Tool in Cyber Warfare by M. KIVIHARJU, The Finnish Defence Forces, FIN
	P-05	Tunneling Activities Detection Using Machine Learning Techniques by F. ALLARD, R. DUBOIS, P. GOMPEL, M. MOREL, THALES Communications, FRA
	P-06	Protected Core Networking - Concepts & Challenges by R. SCHUTZ, THALES Communications, FRA
	P-07	Intrinsic Information Properties by I. BRYANT, UK Ministry of Defence, GBR
	P-08	Extension of the Genetic Algorithm Based Malware Strategy Evolution Forecasting Model for Botnet Strategy Evolution Modeling by N. GORANIN, A. CENYS, J. JUKNIUS, Vilnius Gediminas Technical University, LIT
	P-09	Secure FAST: Security Enhancement in the NATO Time Sensitive Targeting Tool by O. CETINKAYA, Y. YILDIRIM, M. FORTIER, NC3A, NLD
	P-10	Authentication and Authorization of users and services in Federated SOA Environmnets – Challenges and Opportunities by B. JASIUL, R. GONIACZ, R. PIOTROWSKI, J. SLIWA, M. AMANOWICZ, Military Communication Institute, Zegrze, POL
	P-11	Anomaly Detection Framework Based on Matching Pursuit for Network Security Enhancement by R. RENK, K. SAMP, ITTI Ltd., Poznan, M. CHORAS, L. SAGANOWSKI, Institute of Telecommunications, UT&LS Bydgoszcz, W. HOLUBOWICZ, Adam Mickiewicz University, Poznan, POL
	P-12	Speaker Verification using SVM by F. RASTOCEANU, M. LAZAR, Military Equipment and Technologies Research Agency, ROM
	P-13	A New Short Signature Scheme With Random Oracle From Bilinear Pairings by S. AKLEYLEK, METU & Ondokuz Mayis University, B.B. KIRLAR, METU & Süleyman Demirel University, Ö. SEVER, METU, Z. YUCE, STM A.S., TUR
	P-14	Security Survey on SCADA and Distributed Control Systems by S. SAGIROGLU, A. OZBILEN, I. COLAK, Gazi University, Ankara, TUR
	P-15	A Processing of OFDM Signals from UAV on Digital Antenna Array of Base Station in Conditions of Jammers by V. SLYUSAR, Central Research Institute of Armaments and Military Equipment of Ukraine's Armed Forces, Kiev, Ukraine

SESSION 3 - Information Security Awareness

14:45	**7**	Hardware Acceleration for Cyber Security by J. NOVOTNY, T. DEDEK, CESNET z.s.p.o., P. CELEDA, R. KREJCI, Masaryk University, CZE
15:10	**8**	Cyber Defence Situational Awareness and Dynamic Risk Assessment by P. LAGADEC, L. DANDURAND, E. BOUILLON, K. WRONA, S. TORRENTE, NC3A, NLD
15:35	**9**	Assessing and Managing Quality of Information Assurance by P. PAL, BBN Technologies, P. HURLEY, Air Force Research Laboratory, USA
15:55		BREAK

SESSION 4 - Security Models and Architectures

16:25	**10**	Extending Mondrian Memory Protection by C. KOLBITSCH, Vienna University of Technology, Austria, C. KRUEGEL, UC Santa Barbara USA, E. KIRDA, EUROCOM, FRA
16:50	**11**	Self-Defence of Information Systems in Cyber-Space. A Critical Overview by M. COUTURE, R. CHARPENTIER, DRDC Valcartier, A. GHERBI, Polytechnique de Montréal, M. DAGENAIS, A. HAMOU-LHADJ, Concordia University, Québec, CAN
17:15	**12**	Information Security in Maritime Domain Awareness by Y. VURAL, M.E. CIFTCIBASI, S. INAN, STM A.S., TUR
17:40	**13**	Virtual Air Gap – VAG1: A Security Architecture for Information Assurance by A. ÖZGIT, METU, Dept. of Computer Engineering, TUR
19:30		HOST NATION RECEPTION for all Symposium Attendees and Spouses/Companions

Tuesday 27 April 2010

08:30		KEYNOTE SPEECH: by Mr Kenneth GEERS, Scientist at the Cooperative Cyber Defence Centre of Excellence Tallin, Estonia (USA)

SESSION 5 - Authorization and Access Control, Cryptographic Protocols

09:05	**14**	SHIVA Summary by E. CUCCIA, CS Systèmes d'Information, FRA
09:30	**15**	Implementing Cross Domain Access Control for SOA Web Services by J. BUSCH, G. HALLINGSTAD, E. BOUILLON, NC3A, NLD
09:55	**16**	Validation of the PCN Concept: Mobility, Traffic Flow Confidentiality, and Protection against Directed Attacks by P. CARLEN, FMV-Swedish Defence Material Administration, SWE
10:10	**17**	On Hierarchical Threshold Access Structures by K. KASKALOGLU, Atilim University, Dept. of Mathematics, F. OZBUDAK, METU, Institute of Applied Mathematics, TUR
10:30		BREAK

SESSION 6 - Security Policies, Verification, Evaluation and Measurements

11:00 **18** Security Evaluation and Hardening of FOSS
by by R. CHARPENTIER, DRDC Valcartier, M. DEBBABI, Concordia University, TFOSS Research Team, CAN

11:25 **19** Systemic Policy Compliance in a Multi-Jurisdictional Defence Program – Defence Suppliers Perspective
by J-P. BUU-SAO, V. TAKANTI, EXOSTAR, FRA, R. VESTER, Netherlands Ministry of Defence, NLD

11:50 **20** Research and Development Projects Launched in Response to the Dynamic Evolution of Internet Security Threats – A Perspective of a CERT Team
by P. KIJEWSKI, M. MAJ, K. SILICKI, NASK/CERT Polska Departament, POL

12:15 INVITED SPEECH:
by Prof. Erol GELENBE, Imperial College, GBR

12:45 LUNCH

SESSION 7 - Data Integrity and Privacy

14:00 **21** Developing a Cooperative Intrusion Detection System for Wireless Sensor Networks
by L. BESSON, P. LELEU, THALES Communications, FRA

14:25 **22** A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Information Objects
by S. OUDKERK, NC3A, NLD, I. BRYANT, Ministry of Defence, GBR, A. EGGEN, R. HAAKSETH, Defence Research Establishment, NOR

14:50 **23** Towards Dynamic Federated Accreditation: Computer-Assisted Policy Compliance Checking and Risk Treatment
by K. WRONA, G. HALLINGSTAD, L. DANDURAND, NC3A, NLD

SESSION 8 - Intrusion Detection, Prediction and Countermeasures

15:15 **24** Using Anticipative Malware Analysis to Support Decision Making
by M. COUTURE, F. MASSICOTTE, Communications Research Center Canada, CAN

15:40 **25** Living with the Enemy: Containing a Network Attacker When You Can’t Afford to Eliminate Him
by S. KNIGHT, P. SMITH, Royal Military College of Canada, D. VESSEYT, Canadian Forces Information Operation Group, S. LEBLANC, Royal Military College of Canada, CAN

16:00 BREAK

16:30 **26** Automated Attacker Correlation for Malicious Code
by T. DULLIEN, E. CARRERA, Soeren Meyer-Eppler Dynamics GmbH, DEU

16:55 **27** Rumour Detection in Information Warfare: Understanding Publishing Behaviours as a Prerequisite
by F. NEL, LIP6-Université Pierre et Marie Curie-Paris6, P. CAPET, T. DELAVALLADE, THALES Land and Joint Systems, FRA

17:20 **28** Combining Trust and Behavioral Analysis to Detect Security Threats
by O. McCUSKER, Sonalysts, Inc., USA, S. BRUNZA, J. GLANFIELD, Dalhousie University, CAN, D. PATERSON, C. GATES, CA Labs., New York, USA, J. McHUGH, University of North Carolina, USA

17:40 SPECIAL BREAK

18:00 CLOSING CEREMONY with the BEST PAPER AWARD