



DELIVERABLE D11.1

Consolidated Dissemination Plan

Title of Contract	Seamless Communication for Crisis Management
Acronym	SECRICOM
Contract Number	FP7-SEC-218123
Start date of the project	1 st September 2008
Duration	44 months, until 30 th April 2012
Date of preparation	2/03/2009
Author(s)	Tomasz Miroslaw, Wojciech Dymowski, Jakub Bruzdinski, Shaun O'Neil, John Stoodley, Aurel Machalek, Oscar Lopez, Miroslav Konecny, Lubos Slovak, Apostolos Founaris, Ivana Budinska, Tria Assia, Udo Payer
Responsible of the deliverable	Bumar Ltd.
Email	tmiroslaw@bumar.com , jbruzdzinski@bumar.com
Reviewed by:	Miroslav Konecny (Ardaco)
Status of the Document:	Completed
Version	1.02
Dissemination level (select)	PU Public

Table of Contents

1 INTRODUCTION	3
2 IDENTIFICATION OF THE TARGET AUDIENCE	3
3 IDENTIFICATION OF DISSEMINATION CHANNELS	4
3.1 Participation in events relevant to the project issue	6
3.2 Workshops.....	6
3.3 Publications in trade, technical/popular press, journals	7
3.4 Internet presentation.....	7
3.5 Liaison with other projects and similar initiatives	9
3.6 Live demonstration	9
3.7 Exhibition	9
4 DISSEMINATION MATERIALS	9
5 DISSEMINATION PLAN	9
5.1 General.....	9
5.2 Detailed	10
5.2.1 QinetiQ.....	11
5.2.2 Ardaco, a.s.....	12
5.2.3 Bumar Ltd.	12
5.2.4 NEXTEL S.A.	13
5.2.5 Universite du Luxembourg	14
5.2.6 Institute of Informatics, SAS.....	14
5.2.7 Graz University of Technology	15
5.2.8 Smartrends, s.r.o.....	17
5.2.9 ITTI Sp. z.o.o.	18
5.2.10 BAPCO	19
5.2.11 CEA LETI.....	19
5.2.12 Hitachi Europe SAS	20
6 SECRICOM CONFERENCES AND WORKSHOPS (FIG. 1).....	22
7 APPENDIX (POSSIBLE CONFERENCEES AND EXHIBITIONS).....	25

1 INTRODUCTION

This document describes the project dissemination and promotion (hereafter called just 'Dissemination PLAN'). The main targets of this activity are:

- spreading the SECRICOM idea all over the Europe and the world further,
- building right relation between producers and users of various communication systems presumably integrated in SECRICOM vision.
- finding partners (future users) for SECRICOM idea

Dissemination is being defined as communication of information produced by the project or by others about the project. Good communication requires:

- conveying a clear and concise message,
- having a specific purpose and methods,
- attention of the audience/receivers,
- adequate strength of the conveyed message,
- suitable techniques (multi-pronged approach) and environment.

The Dissemination Plan includes the following elements:

- identification of the target audience,
- identification of the most suitable channels for dissemination purposes;
- description of dissemination materials.

2 IDENTIFICATION OF THE TARGET AUDIENCE

SECRICOM is proposed as a collaborative research project aiming at development of a reference security platform for EU crisis management operations. End users of the project solution will be mainly emergency responders (rescuers, fire brigades, special forces, police, etc.), and healthcare providers, even though there exists certain potential in the mass market as well. People/companies/organisations which project issues are of their business constitute the target audience for the project's dissemination activities.

The main project target group constitute first responders:

- governmental services like state police, professional fire brigades, first-aid, ambulance
- city and public services like city police, local crisis management service
- emergency state services like: gas, electricity, water and sewage service

- international humanitarian organization such as Red Cross, Red Crescent etc.
- volunteer rescuing services like volunteer fire brigades, citizens guards
- companies/organizations acting in that field.

SECRICOM has an ambition to keep contact with academic environment, research centres engaged in subject related to the project issue. . It will share valuable results and certain reports with FP7 community potentially interested in security communication area.

It would be valuable to disseminate project results to global business companies, especially construction companies performing work outside commercial communication infrastructure. Moreover it can be presented to private security companies.

3 IDENTIFICATION OF DISSEMINATION CHANNELS

Sources of public outcomes are listed below.

No.	Source
1.	work shops for governmental services newspaper/magazine/journal
2.	conferences dedicated for security and communication
3.	exhibitions of security and defence systems
4.	magazine/journal papers
5.	Internet : <ul style="list-style-type: none"> • webpage • newspaper • newsletters • television / radio / broadcast • specialized webpage • forum • virtual conference • discussion group • virtual archives • mailing list
6.	radio broadcast
7.	meeting and Presentation
8.	leaflet
9.	monographs and publications
10.	ec documents

The main dissemination activities of project include:

- maintenance and population of the project's *website*, where the appropriate information related to the project is placed, as well as project's results, databases and information about the most important events;
- participation in events of relevance to the project (like conferences, fairs, conventions, etc. which the consortium finds useful for the project's dissemination purposes) and promotion of the project through presentations, posters, hand-outs and fliers;
- specific technical *Workshops*;
- *publications* in sectoral and popular press, journals;
- *liaison with other projects and similar initiatives* – to identify the state-of-the-art, promote project results, transfer good practices, and provide end-user view on possible directions;
- promotion and use of the project's results via *other projects* and in day-to-day contacts with potential users and other parties of possible interest.

The above dissemination channels have been listed in the descending order of their significance from the point of view of dissemination efficacy. A number of different factors have been taken into consideration to build the hierarchy, e.g.:

- coverage: sectoral, geographical
- number of entities addressed,
- depth of communicated message,
- availability of the message for target groups,
- independence from external factors;
- cost vs. quality.

It is undisputable that the project should aim at achieving the maximum possible coverage – both from the sectoral and geographical points of view. For this purpose, project partners will use Internet, large conferences and press publications for dissemination, as defined in their individual plans described in the DoW.

For target users' satisfaction, the project should be able to provide information on a continuous basis, so as to avoid "message gaps". This assumption is best met by maintenance of a comprehensive project website. It is the project's most important dissemination means, to be maintained and updated throughout its whole duration. It gives the easiest access to project material and the primary way of communications with the target groups. Still, website's character makes it a rather general source of information, events and direct work with multipliers are foreseen as a much more focused approach for the specific dissemination means. ARDACO is responsible for the project web site. ITTI will support updating information on the SECRICOM web site. ITTI will

place also information about SECRICOM project on the company website. ITTI will provide to the website the information and promotion content related to its responsibilities within the project;

3.1 Participation in events relevant to the project issue

The dissemination activities include the presentation of project results at events suitably relevant to project issue, i.e. seminars, conferences, fairs, conventions etc.

It has to be underlined that dissemination activities, including the participation in project-related events, are less intensive in the first phase of the project and will rise in intensity as the progress in the project is made and new results achieved.

The schedule of fairs, conferences, seminars relevant to the project issue for next year is placed in the Appendix, proposals for simulator promotion (most of those events take place annually, some of them in two year regularity)

SECRICOM project will be presented by Partners during selected events, also via events organized by Forum for Public Safety Communication (PSC). PSC Europe focuses on convergence, at global level, of requirements of Users, Industry, Standard Design Organisations, Research and on seeking agreements on ICT issues related to Public Protection and Disaster Relief. The Forum actively promotes initiatives on these issues and foster discussions through different type of activities.

3.2 Workshops

There will be organised two types of workshops in the SECRICOM project:

1. **Workshops for future users** (crisis management officers, the police, fire brigades etc.) can be organised at the initial/intermediate/final stage of the project. It is suggested to organise meetings every 6 months and invite employees of Crisis Management Centre, fire brigades, special forces, police, TOPR, GOPR (rescues in the mountain area), WOPR (water rescue), MSR (water rescue for Mazury Polish area), rescuers, counter-terrorists, soldiers, civil guards. The end users group is very broad, that is why it is very important to use every opportunities e.g. events were those groups appears.

2. **Workshops for technical specialists** where most feature topics will be addressed. The audience of these workshops will consist of consortium members technicians and invited specialists who can take a role of technical opponents in discussions. These technical workshops will consult key factors of the project. During the dissemination plan preparation was identified first topic – security - that will be covered by technical workshop organised by CEA LETI. Other topics will be identified later.

3.3 Publications in trade, technical/popular press, journals

The written word in hard-copy is another means to publicise project material. Technical and mobile business related journals are prime examples of such a means. SECRICOM participants search for the best opportunity in the country where a text related to the project subject matter could be published (papers, journals relevant to the project issue).

The publications suppose to be regularly put on the project website.

3.4 Internet presentation

The project website www.secricom.eu is one of the main dissemination means, and integrates different means for electronic promotion. The electronic portal will not only serve for dissemination, but also will provide the necessary communication infrastructure to link different simulator-related projects. ARDACO is responsible for the project web site. Partners will support updating information on the SECRICOM web site. All partners should place a link to the project portal on the company websites (with short information about project and project logotype).



The screenshot shows the SECRICOM project website. The header includes navigation links: HOME, PRESENTATION, LOGIN, and the SECRICOM logo. The main banner features a globe and the text "SECRICOM Seamless Communication for Crisis Management".

SECRICOM Project

- Demand
- Objectives
- Project structure
- Expected results
- Funding scheme

CONSORTIUM

- List of members
- Roles and responsibilities
- Business development
- Contacts

Events

- Project events
- Related events
- Presentations

Project DELIVERABLES

- Progress in work
- Public deliverables
- Technical publications

SECRICOM Infrastructure

- Chip-level security
- End-to-End encryption
- Interconnectivity
- Restorable connection
- Smart agent infrastructure

News


Kick off meeting took place in Brussels

On 23rd and 24th September 2008, the Kick Off Meeting of the European collaborative project SECRICOM took place at Sheraton Hotel in Brussels. More than 25 researchers and project managers met to outline the project principles and to set up the work plan for the following 44 months of research. 13 project partners come from United Kingdom, Germany, France, Poland, Spain, Slovakia, Austria, and Luxembourg.

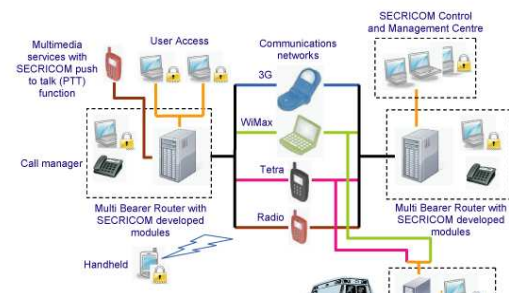
[Read more...](#)

SECRICOM project started

The SECRICOM project started on 1st September 2008. After 458 days since submission of project proposal (30th May 2007) the consortium and EC were able to close the negotiations phase and to sign the grant agreement. The GA



Seamless Communication for Crisis Management

<p>SECRICOM Project</p> <ul style="list-style-type: none"> • Demand • <u>Objectives</u> • Project structure • Expected results • Funding scheme 	<p>Objectives</p> <p>Solve problems of contemporary crisis communication infrastructures:</p> <ul style="list-style-type: none"> • Seamless and secure interoperability of existing many hundred thousand mobile devices already deployed • Smooth, simple, converging interface from systems currently deployed to systems of new SDR generation • Creation of pervasive and trusted communication infrastructure, bring interconnectivity between different networks • Provide true collaboration and inter-working of emergency responders • Seamlessly support different user traffic over different communication bearers <p>Add new smart functions using distributed IT systems based on an SDR secure agents' infrastructure:</p> <ul style="list-style-type: none"> • Easier instant information gathering and processing focusing on emergency responders main task – saving lives. 	<p>News</p> <p>Kick off meeting took place in Brussels</p> <p>On 23rd and 24th September 2008, the Kick Off Meeting of the European collaborative project SECRICOM took place at Sheraton Hotel in Brussels. More than 25 researchers and project managers met to outline the project principles and to set up the work plan for the following 44 months of research. 13 project partners come from United Kingdom, Germany, France, Poland, Spain, Slovakia, Austria, and Luxembourg.</p> <p>Read more...</p> <p>SECRICOM project started</p> <p>The SECRICOM project started on 1st September 2008. After 458 days since submission of project proposal (30th May 2007) the consortium and EC were able to close the negotiations phase and to sign the grant agreement. The GA entered into force on 1st September 2008.</p> <p>Read more...</p>
<p>CONSORTIUM</p> <ul style="list-style-type: none"> • List of members • Roles and responsibilities • Business development • Contacts 		
<p>Events</p> <ul style="list-style-type: none"> • Project events • Related events • Presentations 	<p>Project DELIVERABLES</p> <ul style="list-style-type: none"> • Progress in work • Public deliverables • Technical publications 	
<p>Related ACTIVITIES</p> <ul style="list-style-type: none"> • EU projects • Associations 	<p>Secure Agents</p>	



Seamless Communication for Crisis Management

<p>SECRICOM Project</p> <ul style="list-style-type: none"> • Demand • Objectives • Project structure • Expected results • <u>Funding scheme</u> 	<p>Funding scheme</p> <p>The SECRICOM project has been selected for funding in the Seventh Framework Programme for research and technological development (FP7). FP7 is the European Union's main instrument for funding research over the period 2007 to 2013. It supports the research-related EU initiatives to boost the European growth, competitiveness and employment.</p> <p>The SECRICOM as a collaborative and integration project has addressed the Security Theme in Call FP7-SEC-2007-1.</p> <p>Total cost: € 12.468.847 EU contribution: € 8.606.791 Start date: 01/08/2008 End date: 30/04/2012 Duration: 44 months</p>	<p>News</p> <p>Kick off meeting took place in Brussels</p> <p>On 23rd and 24th September 2008, the Kick Off Meeting of the European collaborative project SECRICOM took place at Sheraton Hotel in Brussels. More than 25 researchers and project managers met to outline the project principles and to set up the work plan for the following 44 months of research. 13 project partners come from United Kingdom, Germany, France, Poland, Spain, Slovakia, Austria, and Luxembourg.</p> <p>Read more...</p> <p>SECRICOM project started</p> <p>The SECRICOM project started on 1st September 2008. After 458 days since submission of project proposal (30th May 2007) the consortium and EC were able to close the negotiations phase and to sign the grant agreement. The GA entered into force on 1st September 2008.</p>
<p>CONSORTIUM</p> <ul style="list-style-type: none"> • List of members • Roles and responsibilities • Business development • Contacts 		
<p>Events</p> <ul style="list-style-type: none"> • Project events • Related events • Presentations 	<p>Project DELIVERABLES</p> <ul style="list-style-type: none"> • Progress in work • Public deliverables • Technical publications 	

3.5 Liaison with other projects and similar initiatives

SECRICOM project wants to work internationally – by raising awareness through international events, or activities. Gatherings organised by other relevant projects are supposed to be monitored by SECRICOM partners. The list of related projects will be updated regularly at the project web site.

3.6 Live demonstration

It is planned to organize three demonstrations to engage users and test their requirements. Two demonstrations of a part system and one final demonstration which will cover part of the scenario and will demonstrate SECRICOM features and benefits against the most important user requirements that are not met by the current communication technology. These presentations will be organized on a training field and special crisis scenario will be played. The location of crisis simulation will exhibit poor communication network coverage. The SECRICOM system will be used to improve coverage and support CRISIS MANAGEMENT COMMUNICATION SYSTEMS. Actors from governmental and volunteer services will be engaged as well as volunteers will be playing role of the potential endangered (victims).

The performance and functionality of the system will be tested. Emergency and public services will be invited to participate in this simulation as testers and spectators.

3.7 Exhibition

Bumar Sp. Z o.o. will provide promotion activity during state and international events all over the world. Bumar has their own trade and marketing activity and participates in many fairs and exhibitions where posters with SECRICOM idea will be presented. The slides with project description and results will be shown in multimedia presentation.

The SECRICOM will be presented as TETRA complementary communication system for Crisis State.

4 DISSEMINATION MATERIALS

Partners will elaborate and develop dissemination material/leaflets informing the public about the aims and results of the project.

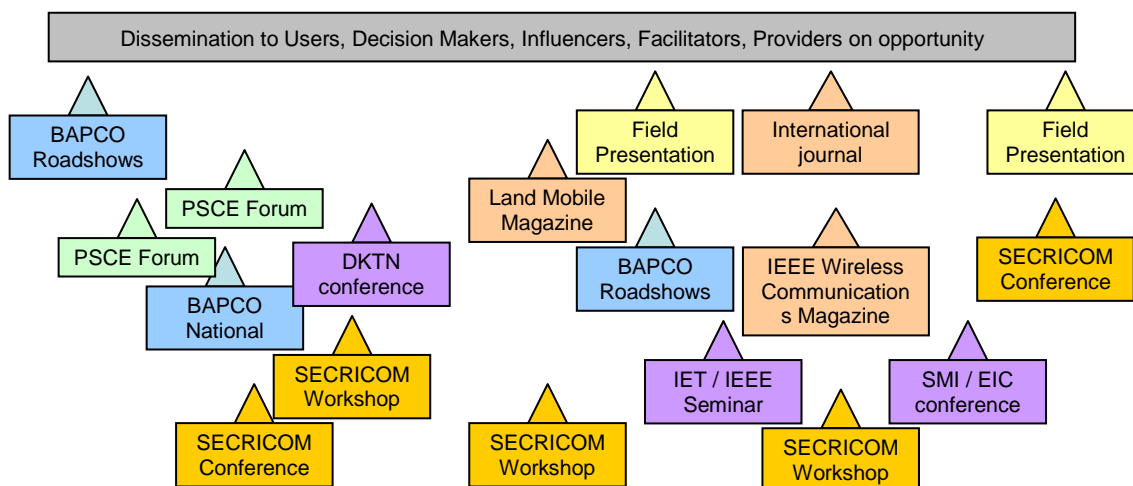
The materials are mainly used for promotion of the project during dissemination events. Virtual promotion is consistent. All mentioned activities will be coordinated by Bumar Ltd.

5 DISSEMINATION PLAN

5.1 General

Dissemination plan follows project milestones and deliverables. It ensures that potential customers and users are updated with the newest achievements and results. Project milestones and general dissemination plan:

-



The list below presents tasks of each partner under dissemination plan for years 2008 – 2010. Each event proposed by partners is placed on the timeline with a corresponding number provided that a date was specified (see *Table 1*). A schedule will be constantly updated whenever a new event is announced.

5.2.1 QinetiQ

The dissemination plan for QinetiQ will include:

- Opportunity briefings to relevant organisations through normal business
- Writing papers for selected publications
- Submitting papers at conferences and seminars
- Supporting SECRICOM workshops and conferences
- Attendance at exhibitions
- Providing 3 field presentations as project deliverables (October 2009, October 2010 and April 2012)

QinetiQ will provide papers for at least 3 publications selected from:

- IEEE wireless communications magazine <http://www.ieee.org/portal/site>
- Land Mobile magazine <http://www.landmobile.co.uk/>
- BAPCO magazine (December issue includes an article on SECRICOM) <http://www.bapco.org.uk/>
- International Journal of Emergency Management
- International Journal of Communication Systems

QinetiQ will provide papers for at least 3 conferences or seminars selected from the following organisations:

- BAPCO National Conference, London (21st to 23rd April 2009) <http://www.bapco.org.uk/events/annual-conference/>
- IET (Institution of Engineering and Technology)
- SMI <http://www.smi-online.co.uk/>
- Event International Conference <http://www.eventi.co.uk/>
- IEEE <http://www.ieee.org/web/conferences/search>
- DCKTN (Digital Communications Knowledge Transfer Network) Sponsored by TSB (Technology Strategy Board) <http://www.dcktn.org.uk/>

QinetiQ will monitor the future conferences organised by IET, SMI, Event International and IEEE to identify any suitable for SECRICOM.

QinetiQ will continue to support the annual BAPCO roadshows having already presented SECRICOM at 3 roadshows in October and will also support the future SECRICOM workshops organised by BUMAR and CEA.

As Co-ordinator, QinetiQ will support the European Commission through occasional briefings as requested by the Project Officer.

As part of normal business, QinetiQ attends selected exhibitions during the year. The exhibitions are selected by the Marketing Director for each Business Sector in agreement with the Business Units. The exhibition plan for April 2009 to March 2010 is due to be published on the 31st March 2009. This is too late to be included in this Dissemination Plan. However, the QinetiQ lead for Dissemination in SECRICOM has identified, in discussion with the Marketing Director, a number of relevant exhibitions that QinetiQ are likely to support and would be relevant to SECRICOM. These include:

- Infosecurity Europe 2009, London (28th – 30th April)
<http://www.infosec.co.uk/>
- Information Assurance (6th and 7th July 2009)
<http://www.iauuk.org.uk/en/Events/Information-Assurance-calendar/>
- Home Office Scientific Development Branch (2010)
- Charing Cross Security Exhibition (2010)

5.2.2 Ardaco, a.s.

- 1) Two papers in referred journals (Computing and Informatics, a Slovak journal in English)
- 2) Three papers in conferences about project proceedings
- 3) Five papers in trade magazines (Computer world in Czech, PC Revue, www.ITNews.sk)
- 4) Conferences (2 national, 5 European, 3 international)
- 5) Presentation at exhibitions and fairs across Europe

5.2.3 Bumar Ltd.

Exhibitions, in which Bumar is going to participate and promote SECRICOM project: (Fig. 2, Fig. 3)

- 1) LAAD, Rio de Janeiro (Brazil)
- 2) Europoltech, Warsaw (Poland)
- 3) SITDEF, Lima (Peru)
- 4) PARTNER, Beograd (Republic of Serbia)
- 5) BRIDEX, Bandar Seri (Brunei)
- 6) DSEI, London (England)
- 7) DEFEXPO, New Delhi (India)
- 8) SOFEX, Amman (Jordan)
- 9) FIDAE, Santiago (Chile)

- 10) DSA, Kuala Lumpur (Malaysia)
- 11) IDEB, Bratislava (Slovakia)
- 12) HEMUS, Plovdiv (Bulgaria)
- 13) EUROSATORY, Paris (France)
- 14) BALT MILITARY EXPO, Gdansk (Poland)
- 15) MSPO, Kielce (Poland)
- 16) BSDA, Bucharest (Romania)
- 17) DEFENDORY, Athens (Greece)
- 18) INDODEFENCE. Jakarta (Indonesia)

There are some magazines listed below, proposals for project promotion (polish press):

- Magazine „W akcji” – <http://www.wakcji.elamed.pl/> ,
- Zeszyty Naukowe AON, Biuletyn AON - http://aon.edu.pl/index.php?option=com_content&task=category§ionid=5&id=3&Itemid=106,
- Kwartalnik policyjny - <http://www.kwartalnik.csp.edu.pl/>,
- Kwartalnik policja - <http://www.wspol.edu.pl/kwartalnikpolicja/> ,
- Armia – Oficyna Wydawnicza KAGERO, <http://kagero.pl/> ,
- Redakcja Wojskowa - Przegląd Sił Powietrznych, Wojsk Lądowych, Morski, Logistyczny, Zandarmerii, Polska Zbrojna, Żołnierz Polski - <http://www.redakcjawojskowa.pl/gazeta/>
- Terroryzm - <http://www.terroryzm.com.pl/index.php?go=kontakt>.

5.2.4 NEXTEL S.A.

- 1) Workshop on Advanced Communication Technologies for Risk, Emergency and Disaster Management 15 September 2008, Cannes, France actRED <http://www.pimrc2008.org/> "Low Cost and High Performance Multi-hop Wireless Mesh Network Solution in Rural and Mountain Areas - Lessons Learnt, Future Challenges and Application to Disaster and Emergency Management", Oscar Lazaro, Innovalia Association [ADHOCSYS]
- 2) Attended to ICT Lyon 2008 (in the role of visitors, participants in workshops discussions related to IPV6 and others)
- 3) Participation and presentations in Company meeting- NEXTEL DAY
- 4) Participation in company Group meeting – INNOVALIA DAY
- 5) Participation in Security DAY organized by NEXTEL and with the assistance of our most important clients

- 6) Article in SIC Magazine (Spanish magazine related with security and communications) <http://www.revistasic.com/>
- 7) Articles in other technological and security magazines, where NEXTEL usually publishes relevant project.

5.2.5 Universite du Luxembourg

- 1) Public Safety Communication - Europe (PSCE) forum in Aix-en-Provence, France (12/2008)
- 2) Creation of the German IPv6 Council <http://www.ipv6council.de>
Creation of the Luxembourg IPv6 Council <http://www.ipv6council.lu> (01/2009)
- 3) IPv6 conference for Luxembourg with the Luxembourg government (01/2009)
- 4) Presentation of Secricom project, UNI.LU with BAPCO in Slovakia, Section of Crises Management and Civil Protection (02/2009)
- 5) presentation of Secricom project, UNI.LU with BAPCO in Luxembourg, Centre de Communications du Gouvernement (03/2009)
- 6) Ethical and Legal issues workshop (03-04/2009)
- 7) Exhibition, E+R+P EMERGENCY+RESCUE-SECUREX+PYROPOL, Bratislava Slovakia, *5th international trade fair of police, security, fire-fighting and rescue equipment* (19-21/05/2009)
- 8) Live demonstration, presentation in Trnava town, Slovakia (16/06/2009)

5.2.6 Institute of Informatics, SAS

Journal papers in

- Science and military. ISSN 1336-8885
- Computing and Informatics, ISSN 1335-9150, www.cai.sk

At least two domestic workshops and two international conferences. We are thinking of:

- 1) WIKT 2009 - Workshop on Intelligent and Knowledge Oriented Technologies, Kosice, autumn 2009
- 2) GCCP 2009 - Grid Computing for Complex Applications, Bratislava, autumn 2009
- 3) National conference "Využitie simulačných technológií pri riešení krízových situácií v MO SR a MV SR" (Application of simulation technology for crisis management)

To this time we have published the following publications:

- 4) BALOGH, Zoltán - BUDINSKÁ, Ivana - ŠIMO, Branislav - HLUCHÝ, Ladislav. Secure management of crisis situations using mobile code in untrustworthy distributed computing environment. In GCCP 2008 : 4th International Workshop on Grid Computing for Complex Problems. Editor

Ladislav Hluchý, Jolana Sebestyénová, Peter Kurdel, Miroslav Dobrucký. - Bratislava : Institute of Informatics SAS, 2008. ISBN 978-80-969202-9-7, p. 113-116.

5) BALOGH, Zoltán - BUDINSKÁ, Ivana - ŠIMO, Branislav. Bezpečné vykonávanie procesov prostredníctvom mobilného kódu v nedôveryhodnom distribuovanom výpočtovom prostredí. In WIKT 2008 : 3rd Workshop on Intelligent and Knowledge Oriented Technologies. Editor Pavol Návrat, Valentino Vranič. - Bratislava : Nakladateľstvo STU Bratislava, 2009. ISBN 978-80-227-3027-3, p. 105-109.

5.2.7 Graz University of Technology

As an academic- and research partners, we will use project-results in our **educational** and **teaching activities**. This includes the design and development of new secure routing protocols, the usage of Trusted Computing (TC) to enable trustworthy virtualization to enable more than one trustworthy compartment, and the design of new hardware solutions (e.g. SDM), to extend the applicability of commonly used TPMs.

Therefore, a set of master courses are offered by the Institute of Applied Information Processing and Communications (IAIK) - covering fields of research wherever we can find points of contact with the SECRICOM project:

- **Advanced Computer Networks** (ACN) is a lecture about modern computer network infrastructures and technologies. The topics of this course ranges from different protocols (IPv6, SCTP, DCCP, ...) over P2P Systems, Voice over IP, Wireless Sensor Networks to hacking techniques and recently exploited vulnerabilities of software or hardware. Beside a theoretical part, a practical part exists, where students will be able to gain first experiences with ad-hoc routing mechanisms and principles based on a P2P middleware, which will be extended during the SECRICOM project. Here we do not start from scratch. Here, we already have a routing framework in use, which is successfully used for more than 2 years in this lecture. But since there are always changes in routing paradigms, we have to keep up with current activities and have to adjust routing requirements to find appropriate solutions.
- **Critical Information Infrastructures** (CII), which is about the use of the Internet and upcoming new risks for critical infrastructures like power supply, telecommunication, and bank services. This lecture gives an oversight of current national and international policies, research and other activities in the field of critical information infrastructure protection.
- **Design and Verification** (D&V) is focussed on advanced methods to test programs, including formal verification. Here, we discuss algorithms for deadlock detection and race detection, program slicing, model checking, and abstraction, which is of immanent relevance in critical information infrastructures (e.g. communication protocols).

- **IT-Security (ITS)**, which is concerned with various forms of applications of cryptography in security protocols, the problem of key management and distribution, the problem of how to implement cryptography in a secure way and how the well known public key algorithms are implemented in practice. In this course, we investigate how to attack a hardware implementation of an algorithm (e.g. on a Smartcard) and we also have a look at various examples of real life scenarios, where an improper use of cryptography lead to security breaks. Real life scenarios--as used in SECRICOM---can help to demonstrate the damage potential of several attacks.
- **Trusted Computing (TC)** is focuses on Trusted Computing as defined by the Trusted Computing Group which plays an essential role in the design of secure agent environments of WP5.
- **Verification and Testing (V&T)**, which is focussed on formal verification, the synthesis of systems from specifications, and their construction.
- **VLSI Design (VLSI)** is about the structured implementation of digital circuits on CMOS technologies. The topic is covered in a top-down approach, where the desired digital functionality is first modelled at high levels and than refined (algorithms, architectures, HDL model) and finally mapped onto a CMOS standard-cell library. Place & route and backend verification ensures manufacturability. In this lecture the background of VLSI design is covered, whereas the practical part of this lecture is planed to be used as a playground for the SDM hardware design.
- **SEMINAR/PROJECT**, is an open seminar-style lecture where we are not limited to predefined topics. Therefore, this lecture is highly suited to give new ideas a trial and to get fast prototypes to be able to make better decisions during the design process.

Moreover, the project will be presented at events organized by the IAIK Trusted Computing Group---most notable is the *ETISS 2009 summer school*---which will be organized by members of the IAIK Trusted Computing Group:

ETISS 2009---the *European Trusted Infrastructures Summer School*--- is scheduled for August 30th-Sept. 4th, and will take place in Graz (Austria). This Summer School will be held together with the TC- and ITS lecture described above.

Furthermore, we plan to submit papers to conferences and journals, within the main research areas: trusted computing, network security and design and verification. A list of adequate conferences is listed below:

1. **MobiSec 2009**, <http://mobisec.org/>
2. **Trust 2009+**, <http://www.softeng.ox.ac.uk/trust2009/>
3. **TrustCom 2009**, <http://trust.csu.edu.cn/conference/trustcom2009>
4. **ISA 2009**, <http://www.sersc.org/ISA2009/>
5. **ITrust 2009** (in preparation)

6. **SASO** 2009, <http://www.saso-conference.org/>
7. **ICUMT** 2009 <http://www.icumt.org/>
8. **CRISIS** 2009 <http://www.crisis2009.org/>
9. **SECURECOM** 2009 <http://www.securecomm.org/>
10. **SENSORCOMM** 2009
<http://www.iaria.org/conferences2009/SENSORCOMM09.html>
11. **SECUREWARE** 2009
<http://www.iaria.org/conferences2009/SECURWARE09.html>
12. **ESORICS** 2009 <http://www.laas.fr/~esorics/>
13. **DNS** 2009 <http://www.dsn.org/>
14. **NDSS** 2009 <http://www.isoc.org/isoc/conferences/ndss/>
15. **CCS** 2009 <http://www.sigsac.org/ccs/>
16. **IWCMC** 2009 " <http://iwcmc.com/>
17. **ETISS** summer school

At present, we have already accepted papers at:

- **SENSORCOMM 2009**, Udo Payer, Stefan Kraxberger, Peter Holzer - "IPv6 Label Switching on IEEE 802.15.4"
<http://www.iaria.org/conferences2009/SENSORCOMM09.html>
- **SECUREWARE 2009**, Stefan Kraxberger, Udo Payer - "Secure Routing for Unstructured P2P Systems"
<http://www.iaria.org/conferences2009/SECURWARE09.html>
- **IWCMC 2009**, Stefan Kraxberger, Udo Payer - "Security Concept for Peer-to-Peer Systems" <http://iwcmc.com/>
- **MOBISec 2009**, Daniel Hein, Ronald Toegl "An Autonomous Attestation Token to Secure Mobile Agents in Disaster Response",
<http://mobisec.org/>

5.2.8 Smartrends, s.r.o

SMARTRENDS' intentions for the dissemination activities include:

1. General dissemination:

Smartrends is a member of couple of initiatives and forums both at the European level and the national level. Smartrends' staff, comprising the Steering Board members of ARTEMISIA and EPoSS, means a number of invitations to various events throughout the year where the SECRICOM project and its latest update will be mentioned in the means of presentation.

2. Publications:

Smartrends intends to publish scientific paper about its results during at the end of the project. The paper will be published in a national magazine in the Slovak Republic which deals with scientific issues and current trends in science.

Smartrends intends to publish conference papers according to conferences foreseen during the lifetime of the project. Although there are many scientific events concerning communication in crisis management going on during one year, usually there is at least one major event to which we will thrive to collect the latest developments of our project results.

3. Internet dissemination plans:

Further dissemination of Smartrends activities will include the short and latest updates of the work progress in the activities that Smartrends is involved. It can be considered as one of the quickest and transparent way of disseminating the project results in a very short time and cost-effective way.

All above mentioned activities are just preliminary intentions and will be updated according to the events being held by the scientific community in the area of crisis management issues. Nevertheless, Smartrends will inform the Work Package Leader about any changes or modifications

5.2.9 ITTI Sp. z.o.o.

ITTI will force to disseminate SECRICOM project via selected web pages from the following (emergency services):

- KGPSP: <http://www.straz.gov.pl/?p=pl/news/>
- GOPR: <http://www.gopr.pl/index.php?grupa=-1>
- WOPR: <http://www.wopr.pl/>
- EUISS: <http://www.iss.europa.eu/index.php?id=155&L=0>

ITTI will force to disseminate SECRICOM project via selected discussion forum from the following (polish forums concerning public, emergency services):

- <http://www.ratmed.pl/forum>
- <http://forum.mswia.gov.pl/>
- <http://www.forum.wopr.net.pl>
- <http://www.pck.pl/forum/index.php?sid=784d30ca16c9c6c0898e7023d5c0b2ee>
- <http://www.strazacy.pl/forum/>
- <http://www.gopr-beskidy.pl/forum/>

5.2.10 BAPCO

- 1) In conjunction with QinetiQ presentations on Secricom's aims and objectives were given at 3 BAPCO road shows (on the theme of interoperability) in the North, Midlands and South of the UK (10/2008)
- 2) BAPCO user team were briefed on the aims and objectives of secricom and then engaged to develop the project scenario (11-12/2008)
- 3) QinetiQ and BAPCO gave a joint presentation on the aims and objectives of secricom to the Public Safety Communication - Europe (PSCE) forum in Aix-en-Provence France (12/2008)
- 4) An article in the BAPCO magazine on Secricom - due for publication March/April 2009; with potential for 6 monthly updates (magazine circulated UK and selectively in Europe)
- 5) An article in the BAPCO E- letter (03-04/2009)
- 6) Presentation at the BAPCO national conference on Secricom in London (04/2009)

5.2.11 CEA LETI

CEA propose to organize annually a workshop dedicated to security. The first one will be organised in autumn (probably in October) in Gardanne. It proposes to cover the following items (relative to WP5 work package)

- Trusted platform module architecture and security
- Embedded security
- Symmetric cryptography
- Fast encryption
- Stream cipher
- Audit processor

We propose to disseminate information about Secricom project in the following media

- Strategy, telecom and multimedia : <http://www.strategiestm.com/-Evenements>.
- Journal reseaux et télécom <http://securite.reseaux-telecoms.net>
- Revue Silicon : <http://www.silicon.fr/fr/news/>
- Revue Global security magazin <http://www.globalsecuritymag.fr>

We forecast to regularly disseminate in the secure competitiveness cluster (SCS) <http://www.pole-scs.org/>

About scientific dissemination we focus to write articles (3 or 4) that can be submitted in the following call:

- ICACNS 2010 : International Conference on Applied Cryptography and Network Security.


- NSWCTC 2010 : International Conference on Networks Security, Wireless Communications and Trusted Computing
- SEC 2010 : IFIP International Information Security Conference
- USENIX Security '10 : USENIX Security Symposium
- TrustCom 2010 : IEEE/IFIP International Symposium on Trusted Computing
- SECURECOMM 2010 : ICST International Conference on Security and Privacy for Communication Networks.

5.2.12 Hitachi Europe SAS

Hitachi will contribute to the dissemination of the Secricom results by submitting, in cooperation with other partners, scientific papers of the Secricom crisis management technical aspects and innovations in international conferences and journal. The primary dissemination objective will be hardware security issues.

More specifically, Hitachi Europe SAS dissemination plan involve submitting scientific articles in:

- at least 3 international IEEE conferences
- at least 2 scientific journals -magazines from at least one of the following publishers:
 - IEEE
 - IET
 - Elsevier Ltd

	DATE																											
	2008				2009												2010											
	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
QinetiQ Ltd.			1 2	3				4		5	6			7				8			9					10		
Ardaco, a.s.									2																			
Bumar Ltd.								1 2	3	4		5	6					7	8 9	10 11	12	13 14			15 16	17	18	
NEXTEL S.A.	1																											
Infineon Technologies AG																												
Universite du Luxembourg				1	2 3	4	5	6	7	8																		
Institute of Informatics, SAS			3	4											1	2												
Graz University of Technology										1,10 11,16			17															
Smartrends, s.r.o																												
ITTI Sp. z.o.o.																												
BAPCO		1	2	3				3	4 5																			
CEA LETI																												
Hitachi Europe SAS																												

yellow – workshops, exhibitions; blue –conferences, presentations; green – publications; red – other

Table 1. Detailed dissemination plan (numbers correspond to events listed in individual dissemination plan of each partner)

6 SECRICOM CONFERENCES AND WORKSHOPS (FIG. 1)

1) Warsaw, Poland ; initial dissemination conference (8th month)

Promoting New Technologies for Crisis Management

Participants: customers and users

2) Gdansk, Poland

Summary conference possibly joint with field presentation (44th month)

Participants: customers and users, beneficiaries



Fig. 2 Exhibitions participated by Bumar Ltd. In Europe

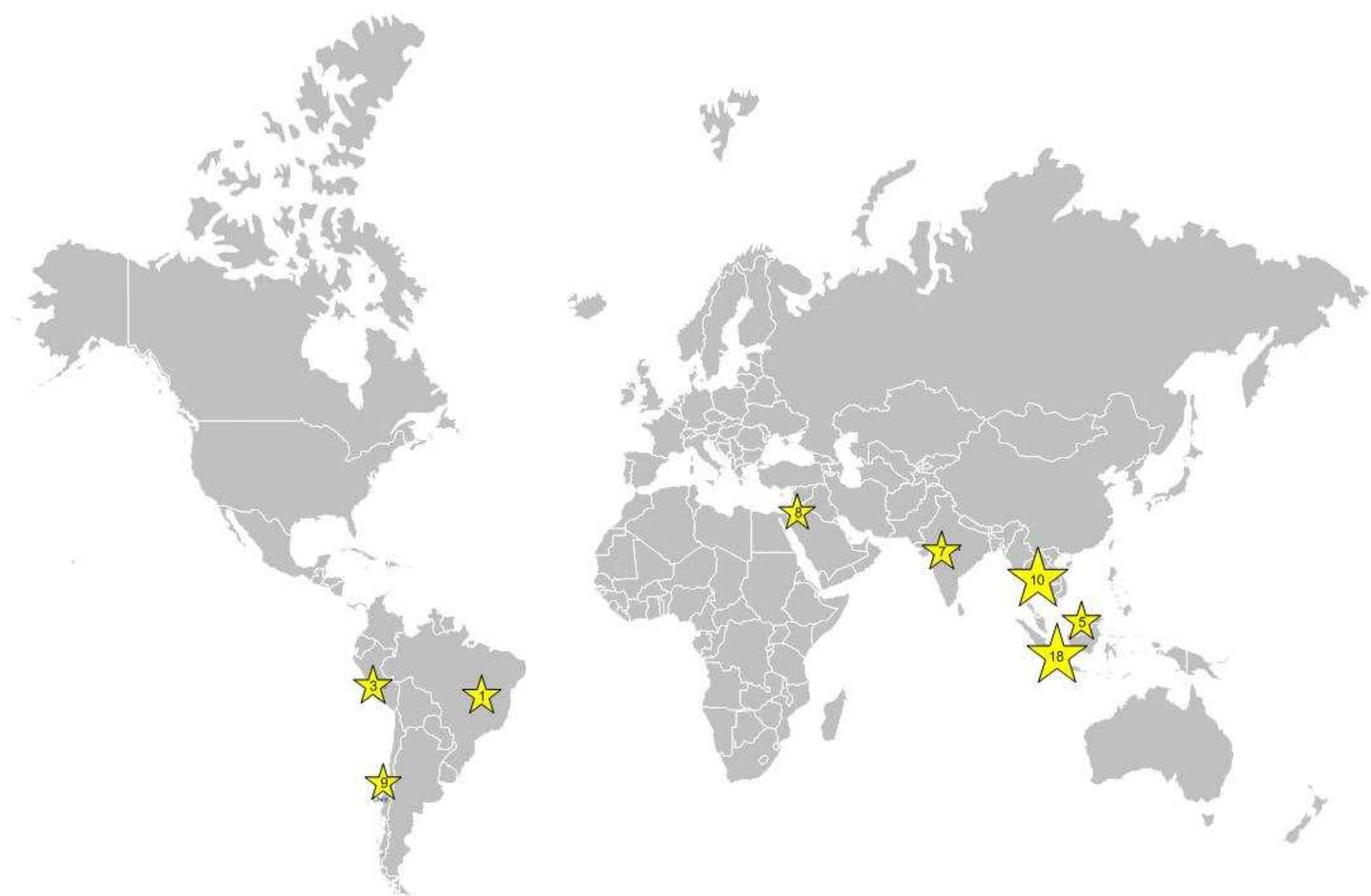


Fig. 3 Exhibitions participated by Bumar Ltd. worldwide

7 APPENDIX (POSSIBLE CONFERENCEES AND EXHIBITIONS)

name of event	when	where	link
IIPSEC 2009	27-29.01.2009	Coventry, UK	http://www.iipseconline.com/home.html
XIV International Forum & Exhibition "Security and Safety Technologies"	3-6.02.2009	Moskwa, Ru	http://www.tbforum.ru/eng/
XIII edycja konferencji z cyklu ZARZĄDZANIE KRYZYSOWE I RATOWNICTWO "SYSTEMY TELEINFORMATYCZNE DLA ZARZĄDZANIA KRYZYSOWEGO W SEKTORZE ENERGETYCZNO - PALIWOWYM"	12.02.2009	Warszawa (CPI), Pl	http://www.cpi.com.pl/imprezy.php
SECURITY	17-20.02.2009	Sofia, Bg	http://www.bcci.bg/fairs/security/
EXPOCHEM	25-26.09.2009	Katowice, Pl	http://www.expochem.pl/
SICUR	26-29.02	Madryt, Es	http://www.ifema.es/web/ferias/sicur/default_i.html
PREWENCJA	13.03-15.03.2009	Szczecin, Pl	http://www.mts.pl/index.php?id=1255
Intertelecom Międzynarodowe Targi Komunikacji Elektronicznej	17-19.03.2009	Łódź, Pl	http://www.mtl.lodz.pl/fair/web/index/id/92
Wystawa Wyposażenia dla Służb Ratowniczych i Policji	19-21.03.2009	Poznań (MTP), Pl	http://www.mtp.pl/all/pl/targi/targi_w_polsce/kalendarium_targow_w_polsce/2009/
VI Konferencja "Wolność i bezpieczeństwo"	april (2009)	?, Pl	last edition: http://konferencje.computerworld.pl/konferencje/wolnosc2008/zagadnienia.html
MIPS	13-16.04.2009	Moskwa, Ru	http://www.mips.ru/eng/

EUROPOL TECH 2009 - Międzynarodowe Targi Techniki i Wypożyczenia Służb Policyjnych oraz Formacji Bezpieczeństwa Państwa	22 -24.04.2009	Warszawa, PL	http://www.europoltech.pl/
The 8th European Security Conference	26-29.04.2009	Montreux, Switzerland	http://www.asisonline.org/education/programs/montreux/default.htm
Infosecurity Europe 2009	28-30.04.2009	Londyn, UK	http://www.infosec.co.uk/
IFSEC 2009	11-14.05.2009	Birmingham, UK	http://www.ifsec.co.uk/
Firex South 2009	12-14.05.2009	Birmingham, UK	http://www.fireandrescueexpo.com/pmfirerescue09/index.html
TIL - Technologia i Infrastruktura Lotnisk	12 -15.05.2009	Kielce, PL	
EDURA 2009 - Międzynarodowa Wystawa Ratownictwa i Techniki Przeciwpowarowej	17 -19.06. 2009	Kielce, PL	http://www.edura.pl/
BALT-MILITARY-EXPO	June 2009	Gdansk, PL	http://www.baltmilitary.pl/
17th International Defence Industry Exhibition MSPO	31 August - 3 September, 2009	Kielce, PL	http://www.targikielce.pl/index.html?k=mspo_en&s=index
15th International Logistics Fair LOGISTYKA	31 August - 3 September, 2009	Kilece, PL	http://www.targikielce.pl/index.html?k=logistyka_en&s=index
SKYDD	September/Octo ber 2009	Stockholm, Sweden	http://www.skydd.net/

Expoprotection	November 2009	Paris, Fr	http://www.expoprotection.com/
SECTECH	November 2009	Kopenhagen, Denmark	www.sectech.dk
ICT 2008 "Europe's biggest research event for information and communication technologies"	November 2009	Lyon, Fr	http://www.enterprise-europe-network.ec.europa.eu/publicwebsite/bemt/home.cfm?EventID=1779
SICUREZZA	November 2009	Mediolan, It	www.sicurezza.it
Infosystem - IT for industry and administration	June 2010	Poznan, Pl	http://www.infosystem.pl
SAWO - Międzynarodowe Targi Ochrony Pracy, Pożarnictwa i Ratownictwa	June 2010	Poznan, Pl	http://sawo.mtp.pl/
SECURITY ESSEN 2008 - The World Forum for Security and Fire Prevention	5-8 October 2010	Essen, Germany	http://www.security-messe.de/?lang=en
CISIS09 - Computational intelligence in security for information systems	September 23-26, 2009	Burgos, Spain	http://gicap.ubu.es/cisis2009