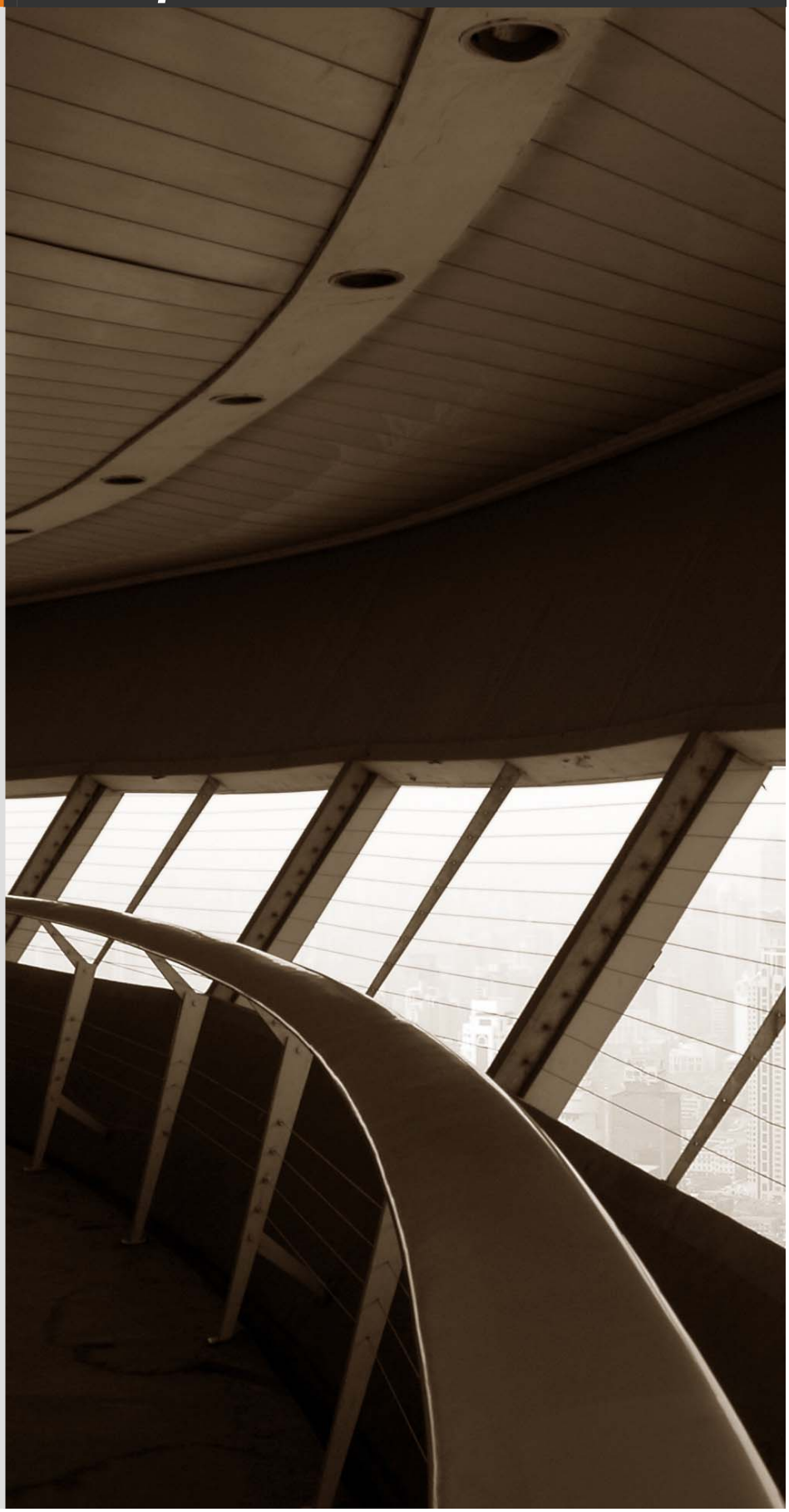
January / February 2006, Volume 2, Number 1

ECN

European CIIP Newsletter



Protection of Critical Infrastructure: EU Homeland Security Association

Survey on CIIP Initiatives in Selected EU New Member States

The Italian Institute for Information and Communication Technologies

Critical Energy Infrastructure Assurance

CIIP Complexity: The Need for a Co-ordinated Research Effort

CI²RCO

> About ECN

ECN is co-ordinated with
The European Commission, Dr. Andrea Servida
For 2005-2006, ECN is financed by the CI²RCO project
The CI²RCO project is an IST FP6 Co-ordination Action,
funded by the European Commission
under the contract no 015 818

>For ECN registration send any email to:
subscribe@ciip-newsletter.org

>Article can be submitted to be published to:
submit@ciip-newsletter.org

>Questions about articles to the editors can be sent to:
editor@ciip-newsletter.org

>General comments are directed to:
info@ciip-newsletter.org

>Download side for specific issues:
http://www.ci2rco.org/

>Founder and Editors
Eyal Adar CEO iTcon, ***eyal@itcon-ltd.com***
Bernhard M. Hämmerli, HTA, Initiator and Main Editor ***bmhaemmerli@acris.ch***
Eric Luiijf, TNO, ***eric.luiijf@tno.nl***

>Country specific Editors
For Germany: Heinz Thielmann, Prof. emeritus, ***heinz.thielmann@t-online.de***
For Italy: Louisa Franchina, ISCOM, ***luisa.franchina@comunicazioni.it***
For France: Michel Riguidel, ENST, ***riguidel@enst.fr***

> Graphics and Layout
Florian Widmer florian_widmer@gmx.net

> Spelling:
British English is used except for US contributions

Table of Content

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

Research and Conferences: Acceptance for CIIP is Raising

This year more conferences on CIIP than ever before will be held. Furthermore the dissemination into many countries in Europe is progressing. New international CIIP research programmes and projects have started and are ready to be launched.

Dr. Bernhard M. Hämmerli

Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
President ISSS / FGSec
bmhaemmerli@hta.fhz.ch
bmhaemmerli@acris.ch

News about Editors

The founding editors have lost Willi Stein. We deeply miss Willi. Our thoughts are with his family.

In this first step we have made a substantial effort to find more country-specific editors collecting contributions from their own countries for ECN. We are therefore very proud to welcome:

Louisa Franchina (Italy)
Direttore Generale
Ministero delle Comunicazioni, Italy

Michel Riguidel (France)
Direktor des Departement Informatique et Réseaux
Ecole Nationale Sup. des Télécommunications, Paris

Heinz Thielmann (Germany)
Former Director of the Fraunhofer Institute SIT and currently advisor on project start-ups internationally.

We are in negotiations with additional country-specific editors in Belgium and Overseas. Our short-term goal is to find country-specific editors form all the advanced CIIP countries and our long-term goal is to include editors from most EU member states, from the United States of America and from Canada in the ECN editorial board.

European Homeland Security Association

We have the privilege to announce the inauguration of the European Homeland Security Association (EHSA) in Brussels. The first EHSA president will be Ambassador Richard Narich presents the actual situation and the EHSA in the lead article of the ECN No. 3.

About Conferences

Italy is very active in the CIIP field. Dr Luisa Franchina is reporting about the conference in Rome in November 2-4, 2005. The next conference CNIP 06 will be held in March 28 and 29, 2006 in Rome. (See article by Sandro Bologna)

The IEEE is also engaged with CIIP workshops: the November 2005 workshop in Darmstadt was very successful (see article by Stephen Wolthusen). In November 2006 in the greater Washington DC area there will be the next Workshop organised by the IEEE's taskforce on Information Assurance within the IEEE Computer Society.

It is a great pleasure to see how conferences and research in CIIP topics have advanced in 2005. It seems that CIIP has progress from long lasting discussions towards an active and focused European CIIP community. We would like to thank all personalities engaging and promoting CIIP!

Authors willing to contribute to future ECN issues are very welcome. Please contact me. Further information about the ECN and its publication policies can be found in the introduction of the first ECN, see www.ci2rco.org.

Enjoy reading the ECN!

Necrology Willi Stein†

The Co-Founder and Editor of the CIIP Newsletter has passed away

Dr. Willi Stein worked for FGAN in the area of information assurance. He took part in NATO R&D working groups and always came well prepared as he collected and studied all literature he could find. This greatly enhanced the scientific basis of these working groups and accelerated the work progress.
In 2002 he took a new challenge in joining the „Bundesamt für Sicherheit in der Informationstechnik, Abteilung kritische Infrastrukturen“ (KRITIS). Soon he collected a lot of publications and other material on C(I)IP. He learned about the Dutch C(I)IP studies and visited The Hague, went to NATO and was one of the experts establishing the NATO/EAPC working group on CIP and the famous NATO / EAPC C(I)IP meetings organised in a co-operation between Switzerland and Germany. He pushed for scientific R&D in C(I)IP and became a CIP lecturer at the University of Bochum.

Willi established a wide network of C(I)IP contacts in many governments and agencies, in industry and universities. He was one of the fathers of the European CIP Newsletter.

He had many ideas how to develop and enhance the C(I)IP area but was diagnose with a brain tumour in early 2005. Medical treatment followed. During his recovery, Willi had a vision how he could drive C(I)IP R&D for the next couple of years.
He could still attend the 2005 CIP conference in Bonn, which he set up in the early stages. He enjoyed meeting all his friends and following all the sessions. It was only shortly afterwards that the illness took away all his and our hope. Willi died at the age of 61 on Friday, 28 October 2005.

We all will remember him as an internationally-oriented, scientific colleague who was deeply interested in humans. We wish Dorothea and the children Andreas and Thomas strength in dealing with their loss.

Eric Luiijf, Eyal Adar and Bernhard Hämmerli

CIIP EU Project IRRIIS is Starting

The Integrated Project “Integrated Risk Reduction of Information-based Infrastructure Systems” (IRRIIS) shall be carried out under the motto: Enhance substantially the dependability of Large Complex Critical Infrastructures (LCCIs) by introducing appropriate Middleware Improved Technology (MIT) components within the next three years. IRRIIS will increase dependability, survivability and resilience of EU ICT-based critical information infrastructures and has the objectives to:

- Determine a sound set of public and private sector requirements based upon scenario and data analysis;
- Design, develop, integrate and test MIT components suitable for preventing and limiting cascading effects and supporting automated recovery and service continuity in critical situations;
- Develop, integrate, and validate novel and advanced modelling and simulation tools integrated into a synthetic environment for experiments and exercises;
- Validate the functions of the MIT components using the synthetic environment and the results of the scenario and data analysis;
- Disseminate novel and innovative concepts, results, and products to other ICT-based critical sectors.

IRRIIS will address the challenges of CIIP by a “diagnosis – therapy strategy” and “therapy implementation and validation approach” starting with the electrical power infrastructure and its supporting telecommunication infrastructure. After thoroughly analysing these infrastructures and their interdependencies, the synthetic simulation environment (SYNTEX) will be build. MIT components will be developed, tested and validated inside SYNTEX to demonstrate their capabilities before dissemination to potential stakeholders. The approach is open for successively including additional critical infrastructures.
The interdisciplinary research will be performed in the coming three years by a European consortium of fifteen partners, ranging from academia to key stakeholders from the fields of energy supply and telecommunication. The project is supported by the European Union Sixth Framework Programme within the area of “Information Society Technologies” with seven million Euro funding and it is co-ordinated by Fraunhofer Institut Autonome Intelligente Systeme (AIS).

Contact: uwe.beyer@ais.fraunhofer.de

Protection of Critical Infrastructure: Importance, Complexity, Results

The point of view of a generalist on an issue more and more relevant to our societies and our citizens.

AMB.RICHARD NARICH

is a career diplomat who served in Latin America as Ambassador (Nicaragua, Paraguay) after being Consul General in Chicago in charge of the Mid-West area. He was assigned in 2001 at the GCSP (Geneva Center for Security Policy) where the French Government regularly sends diplomats of Ambassadorial rank as special adviser to the Director. In the last three years he has been dealing mainly with new security issues, including critical infrastructure protection. He has just been appointed as President of the European Homeland Security Association in Brussels. Mr. Narich is also an adviser to the director of the "Institut National des Hautes Etudes de Sécurité" in Paris and a member of the Board of the French High Committee on Civil Defence.

http://www.hcfdc.org
http://www.e-hsa.org

1. Importance

The need to protect critical infrastructure is not a new development. Natural disasters and human mistakes, capable of causing great damage, have always been of concern to politicians, enterprises and populations. In the case of conflict, infrastructure has also been a primary target for the aggressor and thus prioritised protection for the aggressed.

Why then has this topic become of primary importance in recent years when dealing with security?

There are two reasons behind this increased importance.

First of all, the technological revolution has brought along with it new risk and must thus be contained. The USA has been a pioneer in this movement since 1997.

Secondly, the 9/11 terrorist attacks in the USA further explain this development.

These two events each individually reflect the increasing interdependence of our modern societies, and by default their frailties.

This complexity, interdependence and frailty are the result of several causes:

- A technical cause, the interdependence of the information networks, which underpin the economic activity.
- An economic cause, namely the privatisation process which developed during the 1990s in various regions of the globe, primarily in Eastern Europe. This led many economic activities which had previously been controlled by the state to emerge in the private sector, which, in turn, provoked a fragmentation of the system and thus the need for coordination.
- A geo-political cause, the process of globalisation which extends beyond borders and creates a greater imbrications and dependence. For example, a given country's critical infrastructure can now be controlled by a neighbouring state. Moreover, the supply chain security depends increasingly on foreign markets.

Consequently, the control and protection of infrastructure has become more and more difficult.

At the same time, populations are reacting to a tangible crisis which appears before them on television screens, adding yet another factor to the equation. These developments are occurring at a time when the world's attention is focused more acutely, and rightly so, than ever before on the devastating consequences of international terrorism, even if natural disasters are a greater cause of destruction. It is therefore not an exaggeration to affirm that the "uncertainty threshold" has considerably grown in our societies over the last few years. Given the current situation, two questions must be raised: Firstly, what is the state of reflection upon these subjects? And, secondly, what measures have been taken or are envisaged to control this new situation?

2. Complexity

Four main points can be outlined when examining the state of reflection on the current situation.
These conclusions are greatly inspired by the excellent report written by Ms. Myriam Dunn and Isabelle Wigert,

which is updated every other year by the Federal Institute of Technology, Zurich in the «International CIIP Handbook».

1. The notion of critical infrastructure is commonly accepted even if the actual definition can vary from a country to another. That notion is also widening and evolving. I will provide two examples.

   a. First of all, infrastructure can be critical because it is important for the functioning of a whole set of activities such as an electrical installation. It thus is called "systemic". However, infrastructure can also be classed as critical because it is symbolical. This was the case in the USA with the World Trade Centre in New York. Further examples could include symbols like the Eiffel Tower or the British Parliament.

   b. Secondly, it is evidently important to protect static infrastructure against all aggression, but also services, physical as well as electronic information flows and the messages that the latter transmit. Indeed, aside from physical infrastructure such as dams, it is becoming increasingly common to mention activities like banking and finance transactions.

2. In addition, to the notion of critical infrastructure protection (or **CIP**), the notion of critical information infrastructure protection (or **CIIP**) is gaining immensely and more weight and importance.

   The protection of dams or nuclear power stations has been the subject of much reflection and action for many years now.

   The protection of information systems is a new concern, and is crucial for three main reasons. As previously stated, information systems are at the heart of all economic activity; they are becoming more and more complex and thus increasingly vulnerable; and, thirdly, the threats themselves are becoming more insidious and effective.

3. Due to the growing difficulty found when protecting these increasingly complex installations and systems, risk analysis is becoming ever more widespread, even if it has yet to be refined. The ambition of the latter is to answer through different techniques the following questions: what possible flaws exist? What is the probability that they will occur? What would the consequences of such be? What can be done about it? What options are available and what inconveniences present themselves in terms of costs, benefits and risk? What impact can management decisions have on future choices?

4. Finally, the question of critical infrastructure protection can be dealt with in several ways: from a technical point of view (for example the security of information systems), from a business continuity point of view (here the emphasis is placed not only on protecting the information systems but also their organisation and the human element), and lastly, from a national security standpoint, with the necessary mobilisation of the concerned government agencies, of the representatives of the private sector and that of civil society.

Despite huge progress much remains to be done in order to improve the present situation

Having said all of this, experts realise that total security is impossible. Consequently, they now prefer to use such terms as robustness or resilience.

3. Practical Results

What is the situation then from a practical point of view? What are governments, societies and international organisations actually doing to protect critical infrastructure?

a. The situation was reviewed, as greatly as possible considering the size of the topic, and an assessment was made by the Geneva Centre for Security Policy in the framework of a relevant conference in October 2003. The conference gathered 186 participants and about 60 speakers from 28 countries.

The latter attempted to explore the subject by including all of the actors from the public sector and private sectors, from research institutes and from international organisations. An analysis of this conference was then published in the February 2004 issue of the French Journal, "Défense Nationale".

These are some of the several conclusions drawn:

- Governments are becoming more conscious and as a result more active. This is particularly evident with the American government whose policy is to encourage other countries, notably in the developing world, to address the issue. However, most of the Western countries are equally committed to protecting their infrastructure.
- The same can be said concerning the European Commission, the G8, and other international or regional organisations such as OECD, NATO, the Council of Europe, the European Economic Commission or the International Civil Protection Organisation, more particularly with reference to the protection of information.
- Co-operation between the public and private sectors is progressively developing through the creation of structures initiated either by

governments, the private sector, or both simultaneously. The strongest examples are those given by Great Britain and Switzerland.

b. Initiatives aimed at protecting critical infrastructure have multiplied in the past two years since that conference was held.

As a result, the commission embarked upon a European critical infrastructure program in October 2004.

A new program reassessing the research centres and previous studies concerning critical infrastructure protection in the European Union has just been launched.

Such faraway countries as Azerbaijan have even requested expertise missions.

Conferences and organised seminars on these questions are more are more common throughout Europe.

These examples only provide a mere sample of the widespread and numerous initiatives which are currently taking place.

c. However, as stated at the Geneva conference in October 2003, international co-operation still remains today largely insufficient. Furthermore, a comprehensive evaluation of national risks in most countries is lacking. Intergovernmental co-ordination is generally quite deficient. The same applies regarding co-operation between the public and private sectors.
Much progress is also needed in communication. Decision-makers further still have a great tendency to confront the future's dilemmas with past approaches. They do not think "out of the box" enough.

d. In short, despite huge progress, much remains to be done.

It would therefore be very useful to re-evaluate the issue as quickly and widely as possible.

At this point in time we are still lacking a single structure which would not only allow for the mobilisation of all information, but also be a forum for the exchange of ideas and experiences and thus benefit us all.

Survey on CIIP Initiatives in Selected EU New Member States

A European taskforce to co-ordinate research and development on critical information infrastructure protection and support of co-operation and CIIP awareness was initiated, and the first CI2RCO work package was completed.

Andrzej Bialas & Barbara Flisiuk

Mr Andrzej Bialas, Ph D, is the Director of ICT Security Centre at the Institute of Control Systems, Chorzow – Poland
Ms Barbara Flisiuk is a member of ICT Security Centre team.

www.iss.pl

The aim of the work package was to create a network of CIIP-related research organisations, initiatives and policy makers within the CIIP research fields. This is the basis for further works aiming at identification of completed, on-going and planned CIIP R&D programmes and projects. Their evaluation, in turn, will provide necessary information to identify gaps in CIIP actions and determine R&D priorities.

The paper deals with CIIP-related initiatives in the selected EU New Member States identified by the Institute of Control Systems (ICS) from Chorzow, Poland, acting as a subcontractor of IABG (Ottobrunn, Germany), the CI2RCO consortium member.

Identification of organisations and their activities – towards building CI2RCO community

Each of the CI2RCO members was responsible for identification of organisations and projects in particular countries. ICS's task within first work package of the CI2RCO project was to identify institutions involved in the protection of critical information infrastructures in four EU New Member States: Estonia, Latvia, Lithuania and Poland. The ICS team was also gathering information on projects and initiatives which are directly or indirectly connected with the safety and security of critical information infrastructures functioning in these countries.

The channels indicated by the CI2RCO consortium were used to identify proper institutions and their activities. As much as it was possible ICS used the contacts it had established in the field of information security while implementing various projects, deployment work, training, technical and scientific conferences, etc. Additionally, some Internet research was done to find out key names, organisations and bodies with respect to CIIP. Finally, ICS contacted ministries, research and development centres, infrastructures, public institutions and authorities, as well as associations, foundations and commercial companies in order to invite them to join the project.

So far research and development institutions have been more active in comparison with other potential POCs.

A very good and quick response came from research and development institutions – out of the thirteen recruited Points of Contact (POCs), then are R&D organisations. These POCs are involved in a number of CIIP-related programmes and initiatives and are willing to support the CI2RCO project both by providing information and disseminating project results. There are several reasons for this. First of all, there is awareness of CIIP-related issues among the scientific community. Secondly, CI2RCO, as a Europe-wide project, has a more favourable position than other initiatives

that are often limited to one country. As an EU project it is also associated with good organisation, reliable funding and long-term benefits. Finally, the members of the CI2RCO consortium are recognised as experts in the field of CIIP which is an important factor in recruiting new POCs.

As for the non-scientific community, CIIP awareness is low and the response to the project (or the lack of response) is disappointing. Infrastructure owners and operators have trouble in understanding their role in CIIP and the benefits they could have. They develop autonomous protection systems avoiding co-operation or information exchange. Still, one has to believe that in the course of the project it will be possible to encourage these sectors to co-operate.

Due to the unfavourable time of the research (summer), time limitations and difficulties in locating proper people in particular institutions, the identification of POCs was not satisfactory enough and it has to be continued. Furthermore, the competences with respect to CIIP are often scattered among many institutions and it is difficult to identify the key ones.

Evaluation

The information about CIIP-related programmes and initiatives collected by means of CI2RCO information forms was then evaluated according to the CI2RCO classification scheme. As the level of details varied from one form to another, it was sometimes difficult to interpret the criteria and topics of the classification scheme with respect to the very basic data provided by some POCs. The method was the following:

- Preparing a table to compile the gathered information,
- Identifying and describing particular programmes and initiatives,
- Assigning channels to all programmes/initiatives,
- Analysing each programme or initiative with the help of the classification scheme.

Out of the 22 analysed programmes and initiatives, 14 are from Poland, 7 from Lithuania, and 1 from Latvia. One of them is co-ordinated by a ministry of the interior; six involve co-operation between different sectors, R&D organisations, public authorities and the government. The remaining ones are developed fully or partly by research and development institutions.

Building the CI2RCO community will be a permanent process and more stakeholders will join the CI2RCO team. New organisations are joining the network of POCs.

As far as the character of the programmes and initiatives is concerned, there are two international conferences, a centre of excellence, an EC preparatory action in the field of security research, three projects developed within strategic governmental/national programmes, a national platform for security systems, a PHARE project, a research group working at a technical university, and a safety committee functioning within an interdisciplinary scientific association. Most projects include research by universities or R&D institutions.

The areas covered by the analysed initiatives include:

- Management of health and environmental hazards including risk assessment of hazardous substances, major chemical accidents, as well as chemical, biological and radiological acts of terror,
- Developing technologies that strengthen the security of the state,
- Developing new systems in the fields of postal services and telecommunications,
- Strengthening capacities of authorities dealing with IT and electronic data security,
- Digital rights management and system security management,
- Development of methodologies strengthening trust guarantees,
- Safety analyses of computerised systems applied to the domains of nuclear energy, electricity transmission and railway systems,
- New and emerging IT-implied risks,
- Enhancing security and safety of technical systems and critical infrastructures,
- Cryptographic algorithms and protocols,
- Building secure information infrastructures based on PKI,
- Risk management and critical information infrastructures security evaluation,
- Secure embedded systems,
- IT development while implementing experimental and theoretical systems researches in high risk critical infrastructure facilities,
- Assessment of complex energy systems risk and reliability; development of management methods,
- Probabilistic safety analysis models,
- Management of beyond design basis accidents,
- Development of supporting tools for security design and evaluation and for security management.

Each programme and initiative was described in terms of the sectors it covers, CIIP-relevant topics and criteria it contributes to, and EU-relevant criteria it fulfils.

The information and communication services sector is the most frequently

covered as 12 initiatives deal with it. The branches covered within this sector are: Internet (6 initiatives), computer networks (8), cyber control (4), large proprietary networks (4), wireless communication networks (3), fixed networks (3). Only one initiative covers mobile telecommunication and radio & satellite navigation.

The second sector is transportation with seven initiatives covering such branches as traffic management systems, air traffic management, railway and road transportation, maritime transport, pipelines, and pollutant transport.

Energy comes next with seven initiatives out of which four focuses on electricity, including power transmission and distribution. Nine programmes concern industry with heightened risk for society and the chemical industry is the prevailing branch here (six initiatives).

Safety and security services are mentioned five times and three of these initiatives deal with civil defence issues.

Basically, all sectors of the classification scheme are covered.

As far as the CIIP-relevance of the projects is concerned, each programme /initiative contributes to all criteria groups of the classification scheme although particular criteria vary from one to another.

Dependability: the criteria that could be adapted to particular projects are integrity (12 initiatives), risk analysis (13), availability (10), addressing the interdependency of CI (9), reliability (8), safety (7) authentication/access control (6), addressing the intra-dependency of CI (5) and confidentiality (4).

Survivability: resistance to attacks comes first (11 initiatives), followed by reducing vulnerabilities of CII (10), damage limitation and mitigation (10), business continuity (8), recognition of attacks and extent of damage (6), intra- and interdependencies (5), critical service continuum (5), crisis management model (3). The remaining criteria are applied three or two times. The only criterion not fulfilled is self healing.

Law enforcement: the prevailing criterion is monitoring the systems (15 initiatives), then come ICT measures protecting society against (cyber)crime (13 initiatives), international political agreements and co-operation between states (7), identification and localisation (6), and dissuasion/deterrence (2).

National security perspective: incident /hazard mitigation is the most frequent (12 initiatives), followed by awareness raising (11), warning (8), alerting (7), recovering/re-mediation (6), emergency management response (5), cyber criminality surveillance, and information policy in emergency/crisis (both 4).

All described initiatives fulfil CIIP criteria in terms of their EU-relevance. The majority are projects of national or international importance involving:

- Harmonisation of approaches and programmes;
- Prioritisation of activities with regard to possible attacks, failures and incidents;
- Best practice transfer;
- Integration of national activities.

They are also EU-relevant in terms of addressing the interdependency of CI and applying similar and consistent threat analysis and regarding failure effects to CI. Due to insufficient information it was impossible to assign the following criteria: support of EU political/strategic objectives and sharing of funding.

Conclusions

As the process of building the CI2RCO co-operation network is still underway, there will be further investigations into CIIP-relevant projects. First of all, the information about the above-mentioned initiatives was verified by means of questionnaires within work package 2. Additionally, the CI2RCO team will be looking for more programmes and initiatives that could contribute to the results of the CI2RCO project.

Once the stakeholders see clearly the benefits of joining the project, the participation will rise.

What can be observed now is that approaching the infrastructures (energy, gas, and telecommunication) will require a lot of effort as these communities have been closed so far.

The scientific community, on the other hand, is open to new initiatives but its representatives are interested in solving particular problems. One of the tasks in the nearest future is to recruit to the network a few key organisations, such as:

- Government bodies responsible for security,
- ENISA national representatives,
- National computer response teams.

The most important issue now is how to encourage national information security co-ordinators that can be the key members of the CI2RCO network.

The Italian Institute for Information and Communication Technologies

A summary of the National and International initiatives and Activities carried out by the Italian Body for the Information and Communication Technologies.

Luisa Franchina, PhD

Luisa Franchina is the General Director of the High Institute for Communications and Technologies in the Ministry for Communications.
She is also Ordinary Member of the Superior Council of the Communications, President of the observatory for the safety of the nets and the safeguard of the communications (inter-ministerial national organism for the safety of the public nets of interconnection and the nets of critical infrastructures), and a Member of the Management Board of the European Agency for Network and Information Security (ENISA).
Among other duties, she is co-ordinator of numerous inter-ministerial committees of regulation negotiation for the TLC sector (quality of the service, anti-spam, surcharge services, standardisation of the safety parameters of the nets, etc.)

luisa.franchina@comunicazioni.it
ISCOM: http://www.iscom.gov.it

The fact that the security level guaranteed from the information and communication networks has a strong impact on the modern Information societies development has been world wide accepted and recognised. Such an impact is perceived as crucial at the political level as well as at a technological level. Most of the innovative political proposals (e-government, e-democracy, etc.) and of the business related initiatives (i.e. e-commerce, t-commerce, e-banking, etc.) are not completely developed due the poor level perceived and/or guaranteed by the information and communication networks. Also the emerging broadcasting technologies, such as the digital TV, could be more effective if they were able to fully and securely exploit the interactive services that involve money transactions or highly sensible data exchange.

Security level guaranteed from the Information and Communication networks has a strong impact on the modern Information society's development.

The implementation of a high degree of security in the information and communication networks is an essential requisite when those networks are in charge of the Critical Infrastructure management and protection, such as energy suppliers, railways and mass communication providers, civil protection and all the other bodies that manage high-critical aspects for the proper functioning of the entire country.

Such issues, that are considered the most important in the information and network security, need to be addressed with proper initiatives both at the political and technical level.

ISCOM

The Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Higher institute for ICT) was established in 1907 as a technical-scientific department belonging to the communication ministry. Its main activity is specifically addressed to ICT companies, government agencies and users and is essentially focused on legislation, experimental activities, fundamental and applied research, specialised training and education in the TLC field.

One of the institute's main missions is its proactive role in national and international law-making activities, in order to ensure greater transparency and better access to services for users, manufacturers and TLC network administrators and alike.

The Italian ministry of communications, and specifically ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie della Comunicazione), is developing initiatives on two different sides: on the first the promotion of the international co-operation, while on the other the development of national initiatives targeted to the creation of a synergic environment between all the operators involved in the ICT sector.

ISCOM International Activities

On the international co-operation side are relevant the initiatives with the USA government, with which a great "view's identity" has been recognised on the ICT security topics and specifically on the necessity to contrast the international terrorism, the cyber crimes and the pornography distributed over the internet. The USA shows a great interest in the politics that the Italian government has adopted for the ICT development. The USA is determined to implement inducement politics aimed to the development of new technologies since they are convinced, as we either, that such development can not be left to the sole private market, otherwise a social difference due to technological gap can arise.

Information Sharing has been universally recognised as one of the most efficient tool to implement trans-national synergies in the network security implementation.

Another worth note initiative is the agreement between the Italian and the Israeli governments aimed to the economic, industrial and technical co-operation development and improvement in the network security sector. Specifically the co-operation will be addressed to encourage effective information sharing on standards and laws on one side and the creation of mixed companies, investments and collaboration on the other. With the aim of speed up the development in the network security area, the two countries have agreed and implemented, wherever possible, specific programs and projects through a joint working group that represents a connection and comparison point and is required to identify and define the activities to be implemented and monitor the completed works.

A similar co-operation agreement is currently on going with the Russian, Chinese and North Africa governments.

Still at the international level, two protocol agreements between the Italian ministry of communications and, respectively, the IBM Italia and Microsoft companies, have been signed for co-operation in the network and information system security area. These protocol agreements represent a starting point for the co-operation between the Ministry and the Information security companies. More secure information and communication networks, crimes contrast, protection of minorities navigating the web, and child pornography fight are some of the topics that are addressed in the agreement.

The relationship with the other European countries is also particularly cared. The determinate will of the Italian ministry of communication and of ISCOM in implementing and making operative ENISA (European Network and Information Security Agency) is starting to produce concrete and considerable results, especially in the Information Sharing area, has been universally recognised as one of the most efficient tool to implement trans-national synergies in the network security implementation.

Last, but not least, an example of collaboration with ENISA is represented by the joint organization ISCOM – Fondazione Ugo Bordoni (FUB) – ENISA of the conference on "NETWORK AND INFORMATION SECURITY: POLITICAL AND TECHNICAL CHALLENGES", held in Rome, 2-4 November 2005. The conference main target was to provide an opportunity to meet and share (positive and negative) experiences to the political subjects and high-level technologists involved in the ICT sector, applying also on trans-national level the fundamental principles of "try and fail" and "lessons learnt" approaches.

Among all the participants, Andrea Pirotti, ENISA's Executive Director, presented the European approach to the network security challenge and Guido Salerno, FUB's General Director, brought the Italian experience on the Information Security network topic. Other note worth is that participants are relevant members of foreign institution and companies such as the Moscow government certificate authority, The Holy Seat, the Finn Ministry of transports and the ministry of communications, the university of Rome, the university of Milan, the chairmanship of the Council of Ministries, ESA, ITU, ESRAB, CENTR, CLUSIT, SINCERT, ENEA, GovCERT, and others.

ISCOM National Activities

At a national level, ISCOM promoted initiatives in the CIIP (Critical Information Infrastructure Protection) area. Specifically, it is carrying out an important venture in the information sharing field. Since almost two years, with the co-ordination of ISCOM, a working group that comprises more than 80 public and private organisations has been established. One of the main tasks of the group is to produce guidelines on specific aspects concerning the relationship between the ICT security and the TLC network security. Such guidelines are aimed to spread to PMI, to private organisation, to PA and to the final user the ICT security culture, such as diverted by real experiences of the organizations that participate to the working group.

In 2004 the first three guidelines have been published, titled, respectively, "The Quality of Service in ICT networks" for ADSL & GSM technologies, "NETWORK SECURITY - From risk analysis to protection strategies" and "NETWORK SECURITY - in critical

infrastructures". These guidelines are available in English on the ISCOM website (www.iscom.gov.it). Currently five new guidelines are soon to be published on the following topics: "Risk Analysis Methodologies", "ICT security Certification", "ICT security & outsourcing relationship", "Emergency and Local Accident Management" and "Quality of Service" for UMTS and wideband networks. Furthermore, ISCOM is the Certification Body for the Information Security (OCSI - Organismo di Certificazione per la Sicurezza Informatica) that manages the national scheme for the certification of the ICT security of the products and systems produced following the Common Criteria (ISO 15408) and ITSEC standards.

Another important ISCOM activity related to security certification is its role as evaluation centre of security, CeVa (Centro di Valutazione della sicurezza) in the range of National Scheme that treats classified data and managed by the National Security Authority, ANS (Autorità Nazionale della Sicurezza). It is also a notified body under the EU directive on radio equipment and telecommunications terminal equipment as well as a competent body and notified body on electromagnetic compatibility. In 2002, ISCOM became the international certification body for the TETRA MoU.

ISCOM runs the post-graduate specialisation school in TLC (which began its activity in 1923), which provides higher education in electronic communication and information technologies, and issues a specific degree. Following an agreement signed with the Engineering Department of the "La Sapienza" University of Rome, the School organizes yearly courses which also include laboratory activities, workshops and internships.

ISCOM also provides technical training and updating courses on electronic communications and information technologies, security, multimedia applications, and quality of service to both Ministry and government staff in general, to enhance their technical know-how and skills. For this reason, ISCOM has established a test centre accredited with the AICA, to issue the European Computer Driving Licence - ECDL.

Thanks to the manifold skills and resources it can rely on, ISCOM takes active part in several European projects for technology development and makes ample use of European funds. Such activities are carried out either independently or jointly with other research institutions, universities and international study centres.

As for Information Society activities, reference should be made to a number of projects, some of which carried out together with the Ugo Bordoni Foundation (FUB) in the field of tele-working, IT security, remote learning and access to communication services for disabled or elderly people.

Thanks to ISCOM's support, over the last few years the Ministry was able to implement a number of initiatives to introduce new technologies and systems in communication networks. For example, several feasibility studies were carried out on the application of new TV and multimedia technologies and services, a feasibility study on the provision of macro-regional numerical satellite TV services and a study for the development of a European satellite system to provide multimedia and interactive broadband services.

Another initiative worth mentioning is the ISCOM's participation in the EU IST (Information Society Technologies) research and technology development project called ATLAS.

ISCOM manages the number attribution database for the national telecommunication network and number portability for GSM and UMTS devices. It also manages the National Reference Clock (NRC) to synchronise the Italian numerical telecommunication network and provides institutional support to those who take part in the calls for proposals for the E-TEN (Trans European Network for TLC) EU program. ISCOM works with several certification bodies to verify and control corporate quality system compliance with UNI EN ISO 9000 standard, is involved in monitoring accredited laboratory compliance with UNI CEI EN ISO/IEC 17025 rules and is a notified body for activities envisaged by legislative decree n. 269 of May 9, 2001.

The last chronological initiative that has been started and is expected to have a great impact on the ICT security world is represented by the minister of communication: On Landolfi, proposal to the council of ministries for technical agency on the information & network security topics. Such agency could represent a research & development collector for all the Critical National Infrastructures, both public and private, and a connection point for all the agencies and technical authorities already established in the other countries and with ENISA.

Concluding, I am proud to state the Italian ministry of communication has proposed and implemented effective strategies to cope with the complex problem of the information & network security, both a national and international level, gathering the estimation of the Italian companies and of the central PA that participate with ever more motivation to the implementation of our strategic targets.

Critical Energy Infrastructure Assurance. A case for international collaboration

The IWCIP 2005 workshop provided a truly international forum for presenting and discussing research in a broad spectrum of critical infrastructure protection and is to be the first in an annual series of workshops.

Dr. Saifur Rahman

Dr. Saifur Rahman is the Joseph R. Loring professor of electrical and computer engineering and the director of the Advanced Research Institute at Virginia Tech. He is also the Division Director of Northern Virginia Engineering Program of the university. He is a Fellow of the IEEE, and a director of the IEEE board. He is serving as the Vice President of the IEEE Publications Board in 2006. Dr. Rahman is a member of the Editorial Board of the Proceedings of the IEEE. He has served on the IEEE Power Engineering Society (PES) Governing Board for five years as the Vice President for Technical Information Services and the VP for Education/Industry Relations. He is also a member-at-large of the IEEE-USA Energy Policy Committee. His research interests include alternate energy systems, infrastructure studies, electric load forecasting and power system planning. He has authored over 300 technical papers in these areas.

A critical infrastructure is defined as an infrastructure or asset the destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation (Dunn and Wigert, 2004). Critical infrastructures are generally understood to include: energy, transportation, water supply, information & communication systems, emergency services, law enforcement, financial services, health care, food supply and high vulnerability industries. While these represent a broad array of needs, there are two enabling services that must be assured for any critical infrastructure to function. These are information and energy without which other infrastructures cannot function. The field of critical information infrastructure assurance (CIIA) has been growing for the last several years, and workshops and seminars are being held around the world to explore ideas, opportunities and solutions. A new field "critical energy infrastructure assurance (CEIA)" is evolving as interdependencies among many critical infrastructures are being identified. The CEIA field needs to be defined, and must receive recognition from the practitioners engaged in this line of work which can take the form of education, training, research and outreach in this field.

A transatlantic agenda is needed to formulate and set research goals and priorities that are driven by CEIA requirements and constraints.

While the network of secure information transmission and retention makes communication possible among various components of the critical information infrastructure, a secure energy service provides the necessary support for their operation. In presenting CEIA as a new field of study, this article attempts to examine its component elements and makes a case for interchange of ideas.

The physical part of the national critical infrastructure is understood to be composed of electricity, telecommunication and transportation networks as seen below. They are interconnected, inter-related and interdependent. While the role of electricity in supplying the connected load is well understood, the building blocks necessary to maintain the security and integrity of the electrical network need to be identified, and their functions adequately evaluated.

The discussion below attempts to identify the inter-relationships of these three components of the critical infrastructure. While electricity is necessary to run the telecommunication, computer and transportation networks, proper functioning of the telecommunication and transportation networks is also necessary for the secure and reliable operation of the electricity generation and its supply system.

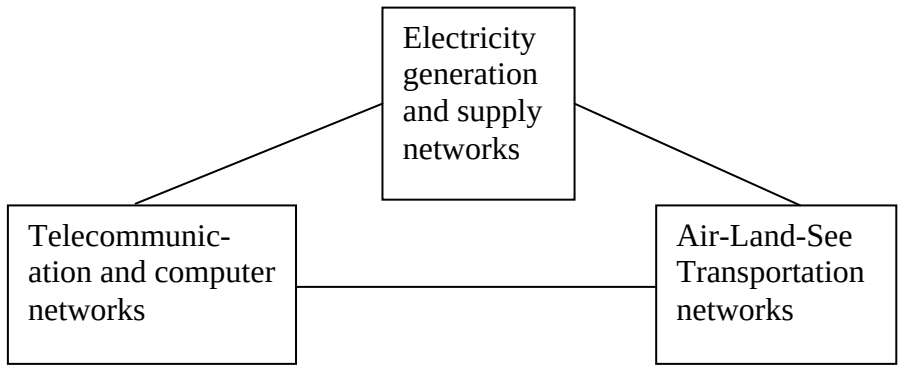


Figure 1: Sectorial Interdependencies

The electrical power system includes generating stations, transmission network and the distribution system. The security of these systems needs to be assured in two different ways – one is the physical and the other is operational. The owners and operators of such systems have their own business practices to ensure the physical security of these systems. There is now a higher level of awareness to strengthen the operational security at the monitoring and control levels for such assets.

One of the integral components in the efficient and secure operation of any of these critical infrastructure systems is the supervisory control and data acquisition system. Commonly known as the SCADA systems, these provide access to local equipment through remote terminal units (RTU) from a central control center. These systems play an integral role in data collection, event monitoring and remote control in various applications including electric power, natural gas and petroleum supply networks, refineries, water supply systems and telecommunication networks. While such systems have a basic architecture that is common across many industries, there are many case specific applications like the design and operation of RTU's, frequency and volume of data collection, intensity of local and regional data processing, etc. In order to understand their unique operations, and the levels of vulnerabilities, it is necessary to study the SCADA practices in related industries, and find common elements across industry groups to focus on resource allocation. For example, in many instances, parts of the SCADA network rely on the public internet to make information easily available to a range of company employees. This opens up the possibility of cyber attacks. Thus it is important to analyze network as well as operating practices to identify new products and software that may have wider applications. At the same time, there are certain industry and application-specific hardware and software designs that need proper evaluation for enhancing system security in the domain of their application. This may lead to identification of gaps in SCADA coverage due to a lack of understanding of the importance of certain segments of the network for system security.

While SCADA systems have been deployed in different industries in various parts of the world, there is a need to understand the differences in the type and level of applications between Europe and the United States. The differences emanate from diverse operating practices including allowable margin of error, acceptable reliability limits and operational norms.

A transatlantic agenda is needed to formulate and set research goals and priorities that are driven by CEIA requirements and constraints. Given the shortage of high-skilled CEIA experts, this agenda should also address training of young professionals and graduate students. One way to make progress would be through joint EU-US workshops or symposia where representatives from industry, government and academia can come together to exchange ideas among a multi-disciplinary group of subject matter experts. The group can adopt an integrated system-level and business perspective to better understand and address the CEIA web of technological, organizational and human factors. It will also provide a forum to explore algorithms, protocols, software, policies and best practices in building dependable energy infrastructures. In addition, such workshops/symposia can help develop a network of researchers and professionals aiming to advance graduate programs in CEIA in both the US and Europe.

References

Dunn M. and Wigert I. (2004) "International CIIP Handbook 2004", Swiss Federal Institute of Technology Zurich.

The Belgian Consultation Platform on Information Security

The consultation platform is a communication forum for all issues relating to information security. The structured, hierarchical nature of the forum means that a solution can be offered for problems that are detected by utilising all the resources available.

Peter Vanvelthoven

Federal Minister of Work and Computerisation

Contact :
De Brandt Remi
Expert
Maria-Theresiastraat 1 – 3
1000 Brussels
0032 2129214

http://www.petervanvelthoven.be

The Consultation Platform for Information Security was approved by the Federal Council of Ministers on 30 September 2005. With this decision, the Belgian government recognised the need to create a platform that plays a co-ordinating role in the field of information security.

It is primarily the permanent members who conduct the deliberations.

The initial experiences of Peter Vanvelthoven in 2003 as the new State Secretary for State Computerisation, made it immediately clear that a great deal of attention needed to be paid to the aspect of information security. “If we wish to retain the confidence of our citizens and companies in our e-government policy, then as a government, we must offer the necessary support,” said the State Secretary as he was then. However, powers in the area of information security have been distributed over various institutions, which were initially assigned with the task of pooling their knowledge and thus creating added value for the federal government.

Gaining the trust of citizens and companies in e-gov policy can only be achieved by maintaining a focus on privacy and information security.

The following permanent members are thus part of the consultation platform:

- **Fedict** (Federal Public Service for Information and Communication Technology) which is responsible for the management of the federal network and also for setting up the building-blocks of the e-gov policy. Increasingly the aim of this department is to computerise all aspects of society.
- The Crossroads Bank for Social Security which manages Extranet, the network of the social security services. Every year vast amounts of data are exchanged via this institution. In addition, it has an information security department providing pragmatic guidance for more than 2,000 institutions.
- The **Belgian Institute of Postal Services and Telecommunication** regulates public networks and other communication channels. Under the new Telecom law, this institution has been granted far-reaching powers in the area of information security.
- The **Federal Computer Crime Unit**. This police unit is empowered to take repressive action against violations of the law with regard to computer crime. In addition to this, using its international contacts it can proactively develop a strategy in collaboration with the other partners. Its responsibilities also include the battle against spam.

- The Crisis Centre. This centre will play a vital role in developing emergency plans for incidents that may endanger the primary government services. The exchange of data means that increasing numbers of emergency services are becoming dependent on these networks for the execution of their core tasks.
- The Commission for the Protection of Personal Privacy. This institution, working autonomously under the guardianship of our Parliament, monitors respect for privacy when using digital resources. It also works proactively by offering advice for proposed projects.

Besides the entities mentioned above, we also have certain services whose core task is to protect the strategic interests of the country:

- The General Intelligence and Security Service. This service, which falls under the aegis of Defence, is responsible for collecting data for the military protection of the country and for Belgians abroad. In the civil domain, the same task is carried out by the State Security Service. The coordination of the authorisations for the security officers, who ensure the protection of information in not only these services but also the other governmental services, is the responsibility of the National Security Authority, in association with the two services above. The task of these services is to protect critical and strategic information. This, certainly in a federal state structure, requires a structured and organised framework. Of course the exchange of security information with other governmental institutions and policy-makers at other levels is of crucial importance here.

And yet there are not only the permanent members ...

When the permanent members decide to work further on a topic, this is taken up by a workgroup. These workgroups, where all permanent members may (but are not compelled to) take part, may request external partners to offer their expertise to the Consultation Platform (e.g. ISPA – the Internet Service Providers' Association, universities, Research Policy, Belcliv, Belnet – the administrator of the federal network, etc.). These workgroups are expected to formulate proposals that offer a solution for the particular problem presented to them. Neither the workgroups, on the one hand, nor the meeting of all permanent members, on the other, have their own decision-making power. The heterogeneity of the permanent members thus requires a consensus, which will not always be easy to achieve. On the other hand if a consensus is reached, it will give the Consultation Platform greater political strength which can only have a positive influence on the implementation of the proposals.

The Consultation Platform can develop its activities as a coordination and knowledge centre. Only then it will prove its strength.

At present three workgroups have been set up:

- Handling botnets (with a denial of service as a consequence). How can action be taken against this?
- Handling the issue of classified information. How can we incorporate the European regulations into our safety regulations? What about encryption? What about approval of hardware and software integrated within crucial applications?
- A third workgroup will involve itself with the concept of "strategic and critical ICT infrastructure". Defining this, and then taking actions based on it, is not always easy.

The Consultation Platform as a coordination centre

Certainly within the framework of classified information, but also for the protection of critical ICT infrastructure, permanent consultation with the regions will be necessary. Therefore in the short term, it is also desirable to include them as permanent partners in the Consultation Platform. In the somewhat longer term, it can be ascertained how the forum positions itself with respect to the local administrations. It is important to have consensus when formulating proposals to present to the federal government. This will demonstrate the strength or the weakness of the Consultation Platform. The organisation is now being finalised in order to be able to work under optimal conditions, and to guarantee that there is good communication between the permanent partners. Indeed the partners have, within their own sphere of influence, complete autonomy. It is necessary to establish a relationship based on mutual trust between the participants but this is something that will undoubtedly take time. Proof of productivity and creativity will greatly increase the credibility of the Consultation Platform. In this way it will become a single point of entry to a general framework for information security. Through the Consultation Platform, the information security regulations imposed by the European Union or supranational institutions can be further extended to the other federal entities, and/or to the regions and the local governments, as necessary.

The Consultation Platform as a centre of knowledge for information security

Information security also has financial implications. It is a rather expensive affair. Here, expertise is paid for in cash. For this reason it is also important that the know-how which is now present in the different institutions is made available to the Consultation Platform. For the government as a whole, this means a win-win situation. In this way government expenditure can be limited.

Nevertheless the government itself will have to invest in information security, if only to retain competitiveness with respect to other countries. Investments in information security are often not made because of a lack of a return on investment. It is only when an actual incident occurs and the damage is assessed that it becomes clear what the investment would have been worth. By then, however, it is too late.

A different initiative: the information security consultants.

Within the network of the social security services, where e-government has already been promoted and implemented for many years now, the institutions are obliged to have a security consultant working for them. The information security service of the Crossroads Bank of the Social Security Service helps to organise this. In this way, a coordinated approach to the required security measures emerges. The objective is that this well-functioning system be implemented in the other sectors of the federal government. The exchange of data with policy-makers at other levels obliges the government to take this measure. The Forum, which is the group of security consultants, will also be linked with the Consultation Platform for Information Security. The Forum will additionally be able to formulate proposals that are directly related to the information security policy of the government, but always with respect for the protection of citizen's personal privacy. "After all, privacy and information security are not contradictory terms," according to the Minister of Work and Computerisation. "We must make sure there is a fair balance so that everyone can carry out his or her task properly and whereby added value can be created for the whole of society."

CIIP Complexity: The Need for a Co-ordinated Research Effort

The vulnerability of our institutions and of man-made structures has become clear. It is necessary to stimulate global research efforts to improve the resilience of infrastructures that offer critical services to citizens in order to protect the states, the companies that operate infrastructures and the citizens themselves.

Dr. Gwendal Le Grand

Associate Professor,
Ecole Nationale Supérieure des Télécommunications, Paris, France,

gwendal.legrand@enst.fr

For years, before communication means became essential to the world's functioning, natural disasters and human errors on an infrastructure had impact on this particular infrastructure only. Thus it was controlled by its own security policy. If digital technology drastically improved human society it did, however, complicate security measures. Today, our society has become increasingly complex and fragile because of its IT[1]-dependency and its interdependent infrastructures. Those interdependencies are global among heterogeneous infrastructures and range from telecommunications to energy, banking, transportation, health, defense and public administration. Although this globalisation of infrastructures aims at improving the service provided to end users, it is nevertheless the source of new vulnerabilities. Therefore, the close relationships between infrastructures can increase the consequences of a fault when they propagate within the infrastructure or to another dependent infrastructure before any mitigation measures could be taken.

THE NEED FOR A GLOBAL APPROACH

CIIP[2] aims at securing information infrastructures and their interdependencies in order to avoid cascading and escalating effects and ensure the survivability of critical services. In order to achieve this and provide a global security vision, one must take into account the technical elements within an infrastructure as well as all the symbolic elements related to this infrastructure. For example, when a telecom infrastructure collapses and users are no longer able to use it, both the business (through profit loss) and the corporate image of the provider are impacted. This will in turn impact the future business of the company and maybe its competitors

For example, in November 2004, one of the three French GSM networks crashed during 20 hours, due to a bugged update of Home Location Registers (HLR). The company had two HLRs for redundancy and improved resilience reasons, but both crashed at the same time because the update was performed simultaneously at both equipments.

Although the technical loss was estimated around 20 million euros (one day of sales turnover), the corporate image impact was estimated (by the operator) up to four times more than the actual profit loss when the company turned the responsibility over to its HLR supplier.

Since it is impossible to design error-free systems due to complexity and interdependencies, today's resilience is often provided a posteriori once vulnerabilities have been exhibited. This GSM breakdown has provoked

[1] Information Technologies
[2] Critical Information Infrastructure Protection

many reactions from the French government, which required a strict investigation. It turned out that the emergency phone number was not accessible during the breakdown because of its connection to the HLR for an authentication that was always granted! Therefore, the crash impacted all the GSM operators that were forced to update their network so as to provide an emergency number always reachable.

COMPLEXITY

It has become very complex to design secure infrastructures today, due to several natural properties that they exhibit like for example heterogeneity, scalability issues, and mobility of the users. In such a boundless world, it seems obsolete to ensure security by setting up access controls on virtual flexible boundaries. Moreover, eagerness to release a brand new product, hardware or software, can be the cause of errors, some that may even prove critical to its survival. Today's communication services allow hackers from the far side of the planet to quickly exploit such vulnerabilities.

Spending excessive time to develop an error free product is unconceivable and only the monitoring of a system's lifecycle may help detect abnormalities. Yet, detection is no cure and it is necessary to come up with new security measures and redundancy where it is needed.

INTERDEPENDENCIES

The weakness implied by the interdependencies of infrastructures will certainly lead to future attacks using the interplay of several infrastructures operating in intertwining functionality, while the attacked infrastructure may not necessarily be the final designated target. The interconnections of these infrastructures will disseminate the effects of such attacks while their dependent structures will cause more serious accidents. The lethal chain of events will then be difficult to predict or control.

In the case of interconnected infrastructures, each infrastructure has its own security policy. Typical attacks on interdependencies cannot be modelled as failures or as one-time events occurring at random. It actually represents a series of targeted events converging on the same objective. Interdependent systems then need additional security measures to be taken if this type of situation is to be eradicated. Therefore, interdependent structures must be considered as whole. If security of interconnected structures can't be realized by securing each sub-structure, the whole entity must be meta-modelled.

Therefore, a global and systemic approach is necessary to grasp all the facets of Critical Infrastructure Protection.

PUBLIC vs. PRIVATE INTERESTS: collaboration is needed

Improving the resilience of interconnected and interdependent infrastructures intuitively leads to the sharing of knowledge, data and intelligence. Yet, if such a security mean is likely to bring better defence against a common enemy, it may initiate new dangers by disseminating company-secret information.

A global and systemic approach is necessary to grasp all the facets of Critical Infrastructure Protection.

Although most infrastructures are owned and operated by the private sector, those infrastructures often provide public services that need to be maintained and regulated by governments. Regional, national, and international activity to protect infrastructures requires creative forms of co-operation in which governments should play a key role. This interventionist vision of the states is often considered by many European members to be a French vision which is possible in France or countries where infrastructures are owned and operated by public companies that have a monopoly. This situation obviously does not reflect today's situation in France even if competition in some domains is not as advanced as in other countries. But more important is the fact that private and public interests converge; private critical infrastructure operators should be convinced that they have to share data and knowledge with other organisations in a trusted and well defined legal context. The European isolationist attitude of infrastructure operators is all the more surprising when one notes how much effort is being made to protect each individual infrastructure.

Even the United States which is usually considered by Europeans as a country with fierce competition and deregulation shares this point of view: "No matter what the United States does to protect itself, we are only as secure as the least secure nation to which we are connected", said Michele Markoff, the State Department's senior co-ordinator for international critical infrastructure protection policy. Therefore, private companies, regional, or even national efforts are not sufficient if the rest of the world remains unprotected. Like the Department for Homeland Security (DHS), European nations should be empowered to organise and frame public-private engagement as a key component of the strategy to secure cyberspace and support technology R&D that will enable the private sector to better secure privately-owned

portions of the nation's critical infrastructure. Although some positive signs can already be seen in some member states or at the European Commission, there is a clear and urgent need in Europe as a whole, for frames in which such collaboration is made possible. It is necessary to investigate all the possible means to enforce this collaboration. Security standards must be developed and the states must be in the position to enforce them; they can impose their rules to the stakeholders if business is only made possible to compliant companies. At the international level, this type of approach is used by the United States that forced other nations to comply with domestic passport regulations on optical scanners and now on biometric identification so that immigration procedures can remain simple.

European nations should be empowered to frame public-private engagement as a key component of the strategy to secure cyberspace

HETEROGENEOUS APPROACHES AND DOMAINS

The main difficulties of CIIP research find their origins in the complexity of the systems, in the number of stakeholders, and in the diversity of domains that are to be considered. For instance, the army or the police contribute to public safety (and thus to the safety of IT experts that operate infrastructures), whereas IT experts improve the resilience of information infrastructures that may in turn contribute to public safety.

Today, it appears that the words "security", "Critical Infrastructure Protection", and "Critical Information Infrastructure Protection" get a lot of hype and are used (and sometimes interchanged) by all the communities that contribute to CIP, even though the methodology (and even the sectors) associated to them varies. Naturally, it is hard to federate efforts when the understanding of the vocabulary and of the priorities is so heterogeneous. However, what could at first be seen as a brake to the effort can also be considered as a major asset if the communities manage to structure their effort. Once again, positive signs of a federated and consistent research effort are visible in member states (for instance, it is the case in France), thanks to the common efforts of the governments (at the national and European level), the academic, and the industries.

SECURITY R&D AT THE NATIONAL LEVEL IN FRANCE

The European Commission is planning to include an important European Programme on Security Research (EPSR) within the Framework Programme 7 (2007-2013). This research programme should be centred on user needs by orienting works towards the realisation of demonstrators. It also has the ambition to stimulate European industrial competition. France believes this will be an opportunity to increase its industry's competition and the excellence of its research laboratories in the security domains. This programme is preceded by Preparatory Actions on Security Research (2004-2006). The keen interest for those preparatory actions motivates the French government to prepare and organise a community from the FP7 point of view. Under the leadership of the SGDN (National Defence General Secretariat), several large scope workshops and a working group have been organized with the participation of major ministries (Research, Defence, Interior, Health, Industry, Transportation, Foreign Affairs). The working group prioritises the needs of the ministries and identifies the technological and industrial stakes related to those needs.

TOWARDS A RESILIENT INFRASTRUCTURE OF INFRASTRUCTURES

Due to the omnipresence of Information and Communication Technologies in our daily lives and from all the efforts and events that are observed at the industrial, academic, national and European level in every member state, it is evident that CIIP has become a major issue of our modern society. People and machinery are working together without any geographical boundaries. However, this global interconnection increases threats and introduces new vulnerabilities.

In this context, national member states and Europe must play a key role to define research agendas and provide a framework and a set of tools to stimulate and foster collaboration and research both at the domestic and at the international level. There is a need for collaboration to identify elements displaying higher vulnerabilities and those that are crucial for the continuity of supply of multiple providers. This will assist the understanding, modelling and gap analysis of interdependencies and their impact on business. The stakeholders must co-operate to define a research agenda and agree on the standards needed. Only then will risk mitigation really be tackled.

In parallel, international collaboration with advanced countries in the field of CIIP should be encouraged.

Employing IPv6 to Improve Layer 3 Defence in SCADA Systems

While SCADA systems that communicate through IPv4 have inherited its vulnerabilities, IPv6 appears as an open research trend and a potential candidate for improving the security of SCADA networks.

Julian L. Rrushi

Dott. Julian L. Rrushi[3] is a PhD student of the Università degli Studi di Milano. He holds a MSc degree in Information and Communication Technology, and a BSc degree in Computer Science from the aforementioned University. In 2005 he was awarded a research scholarship by (ISC)², and an internship by the Joint Research Centre of the European Commission. He is a member of the European Security and Dependability Task Force.

julian.rrushi@jrc.cec.eu.int

SCADA (Supervisory Control and Data Acquisition) systems are used to monitor and control in real-time both local and geographically remote distributed processes.

Generally they consist in a system controller referred to as master terminal unit, which issues commands to distant facilities referred to as remote terminal units, which in turn control or acquire data from field devices.

The network version of modern SCADA protocols such as DNP3 and IEC 60870-5-104 currently run over IPv4, a protocol that has left the layer 3 attack resilience an open research issue.

Hence a master terminal unit may instruct a remote terminal unit either to open or close valves, turn switches on or off, etc., or send real-time data collected from various sensors on the field.

The need for a fortified layer 3 in SCADA networks

As SCADA systems are deployed in industries such as electrical power grids, transportation, water control, oil and gas refining, etc., their protection from physical and cyber attacks is of paramount importance to a nation's security, especially taking into account eminent threats deriving from actualities such as cyber terrorism, defined as a convergence of terrorism with cyberspace [4].

Originally supervisory control and data acquisition protocols used to run over low bandwidth bit-serial communication circuits. With the evolution of networking technologies, these protocols have been extended to create their network version, which provides support for communications over TCP/IP or UDP/IP [3].

Modern SCADA networks comprise LANs (Local Area Networks) and WANs (Wide Area Networks). In fact a master terminal unit is usually connected with some administrative systems in a LAN, and the SCADA systems themselves are connected to the whole corporate intranet.

Furthermore, SCADA systems are sometimes connected even to internet for reasons such as allowing remote viewing of real-time data or getting technical support from remote centres. Thus, in front of such a relatively high connectivity, a layer 3 protocol that is weak from the security point of view could enable an attacker to mount devastating attacks against SCADA systems from so many points.

The impact of IPv4 insecurities on SCADA networks

The network version of modern SCADA protocols such as DNP3 and IEC 60870-5-104, used for communications between master terminal units, remote terminal units and field devices, currently run over IPv4 [12], a protocol that has left the layer 3 attack resilience an open research issue.

As the IPv4 header has no security mechanism itself, its security relies on IPsec [13]. But IPsec suffers from issues

[3] The information reported in this document is that of the author and does not necessarily represent an official position of the Joint Research Centre of the European Commission

such as complexity [10] and key management, just to name a few, and until they are resolved deployment of IPsec will be stalled [5].

In a SCADA IPv4-based network an attacker could spoof IPv4 addresses and mount layer 3 attacks such as broadcast amplification where possible, routing protocol attacks that disrupt or redirect communications between SCADA systems, or communications between those SCADA systems and other systems in the corporate intranet, etc.

The real security advantages of running the network version of SCADA protocols over IPv6 consist of continuous improvements in the security of IPv6, and the security research trends that IPv6 represents.

Furthermore, in a SCADA IPv4-based network an attacker could try to manipulate bindings between IPv4 addresses and link layer addresses by attacking ARP (Address resolution Protocol) [9], and redirect SCADA protocol traffic through his machine. This attack is known as MITM (Man In The Middle).

In the case a DHCP server is used, an attacker could generate DHCP messages with spoofed information causing victim nodes to get configured with incorrect network information.

While this paper does not pretend to provide an exhaustive discussion on layer 3 threats deriving from weaknesses in IPv4, there are no doubts on the fact that the network versions of SCADA protocols have inherited the exposure to those threats. Furthermore, IPv4 spoofing opens the way to attack attempts against TCP, and this affects directly the network version of SCADA protocols as they run exactly over TCP/IP.

As a matter of fact a TCP session is identified by a coupling of a socket on the client and another one on the server. Thus, a TCP session is identified by: (client IP address, client TCP port; server IP address, server TCP port) [11]. If the attacker can spoof IP addresses and TCP ports, and uses a sequence number acceptable to the victim(s), he can hijack or disrupt TCP connections.

The ability to spoof IPv4 addresses enables an attacker to try to take over TCP connections that either originate from or are destined to SCADA systems, by carrying out local session hijacking attacks in the case that attacker can sniff the network and learn the correct sequence number to be used in the attack packets, or blind session hijacking attacks otherwise [16] [17].

Spoofing IPv4 addresses enables an attacker to also try to disrupt those TCP connections by carrying out denial of service attacks such as reset [19] or TCP syn flood [18] ones.

Could a SCADA IPv6-based network have better defensive capabilities?

The security features of IPv6 [1] and its resilience to various attacks had been clearly identified by the research discussed in [5], concluding that IPv6 security was in many ways the same as IPv4 security. Just like the IPv4 header, the IPv6 header has no security itself, thus it relied on IPsec too.

Despite this, significant results have been achieved by ongoing research. To the author's opinion the real security advantages of running the network version of SCADA protocols over IPv6 consist in continuous improvements in the security of IPv6, and the security research trends that IPv6 represents.

It is true that initially IPv6 addresses could be spoofed as easily as IPv4 ones, and IPv6 protocols suffered from vulnerabilities similar to those of IPv4, but the situation changed.

As an example, within a European project called 6NET [14] we experimented with a variety of attacks against the Neighbour Discovery Protocol [2] in a native IPv6 network at the Università degli Studi di Milano, and results were reported in [7].

By practically implementing attacks based on spoofing, and distribution of bogus information, mainly operating on parameters such as prefix, maximum transfer unit, current hop limit, and router lifetime, we practically verified the possibility to hijack or disrupt IPv6 traffic, and even bring entire sub networks to a halt.

In a SCADA network using protocols in that status, an attacker could have the possibility to use a system connected to the SCADA network and that he controls, a rogue machine he connects to the SCADA network in question, or even a compromised SCADA system, to affect SCADA communications or take down the whole SCADA network. He could also operate from the corporate intranet or even from internet if he can.

A significant achievement in securing IPv6 protocols has been the invention of CGA (Cryptographically Generated Addresses). CGA are IPv6 addresses whose rightmost 64 bits are generated by computing a cryptographic hash from a public key and auxiliary parameters [6]. Thus, a binding between a public key and an IPv6 address is created.

CGA does not allow spoofing of IPv6 addresses; hence all those attacks against a SCADA network mentioned above could be blocked. Furthermore, CGA does not require a certification authority or a security infrastructure. However, as SCADA systems act in real-time, they need to be fast.

Thus, careful measurement of the cost of operations such as calculating the cryptographic hash from the public key and auxiliary parameters and using it to create a CGA, verification of the association between the IPv6 address and the public key, or signing with the private key the messages sent from that IPv6 address, should be carefully performed in a SCADA system and taken into account.

There are still many IPv6 security research issues that deserve investigations in depth, and which could open new frontiers in the defence of Critical Infrastructure networks.

A SCADA IPv6-based network would not be exposed to broadcast amplification attacks, as ICPMv6 [15] takes special measures to protect the network from them.

In the case an attacker does not have the possibility to spoof IPv6 addresses any longer, MITM attacks against the Neighbour Discovery protocol, which is the IPv6 equivalent of ARP in IPv4, are not possible. Furthermore, in the case a DHCPv6 server is used, an attacker could not generate DHCPv6 messages with spoofed information

When the network version of SCADA protocols runs over an IPv6-based network that is protected from spoofing of IPv6 addresses, an attacker could not be able to inject attack packets into a TCP session. This is because the source IPv6 address of those attack packets cannot be the IPv6 address of one of the legitimate communicating parties, therefore the sockets identifying that session would invalidate them.

Furthermore, novel IPv6 security features must be explored so that to address each one of the steps in the anatomy of a hack [8]. Despite significant improvements, there are still many IPv6 security research issues that deserve investigations in depth, and which could open new frontiers in the defence of Critical Infrastructure networks.

Conclusion

The layer 3 defence that IPv4 provides to the network version of SCADA protocols is not robust enough to stop many devastating network attacks. A more secure layer 3 protocol is needed especially for networks such as SCADA ones that often constitute the heart of a nation's life supporting industries.

A potential candidate that could provide an adequate protection to SCADA networks is IPv6. Initially the security of IPv6 was the same as that of IPv4, as it relied on the use of IPsec. However, IPv6 security got improved, and significant results are reported by ongoing research. Many known attacks have been addressed by novel IPv6 security approaches, and many interesting research issues are open for further investigation.

IPv6 has much to offer to the defence of Critical Infrastructure networks, and future research could find in IPv6 a lot of valuable security features that characterize a good layer 3 protocol.

References

[1] Deering S., Hinden R., "Internet Protocol, Version 6 (IPv6) Specification", RFC-2460, December 1998.

[2] Narten T., Nordmark E., Simpson W.A., "Neighbor Discovery for IP Version 6 (IPv6)", RFC-2461, December 1998.

[3] Clarke G., Reynders D., "Practical Modern SCADA Protocols", 2004.

[4] Denning E., "Cyberterrorism", Global Dialogue, 2000.

[5] Convery S., Miller D., "IPv6 and IPv4 Threat Comparison and Best Practice ", March 2004.

[6] Aura T., "Cryptographically Generated Addresses (CGA)", RFC-3972, March 2005.

[7] Rosti E., Rrushi J.L., "IPv6 Neighbor Discovery Protocol: A Security Case Study", In Proceedings of the IADIS Applied Computing Conference, pp 313-320, Portugal, Febbruary 2005.

[8] McClure S., Scambray J., Kurtz G., "Hacking Exposed, Network Security Secrets & Solutions", 4th edition, 2003.

[9] Plummer D.C., "An Ethernet Address Resolution Protocol", RFC-0826, November 1982.

[10] Ferguson N., Schneier B.,"A Cryptographic Evaluation of IPsec" , Unpublished manuscript, February 1999.

[11] "Transmission Control Protocol", RFC-793, September 1981.

[12] Postel J., "Internet Protocol", RFC-0791, September 1981.

[13] Kent S., Atkinson R., "Security Architecture for the Internet Protocol", RFC-2401, November 1998.

[14] The 6NET project, http://www.6net.org

[15] Conta A., Deering S., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC-2463, December 1998.

[16] Joncheray L., "A Simple Active Attack Against TCP", In Proceedings of the Fifth Usenix UNIX Security Symposium, Salt Lake City, 1995.

[17] Bellovin S.M., "Security Problems in the TCP/IP Suite", AT&T Bell Laboratories, 1989.

[18] Rodgers C., "Threats to TCP/IP Security", 2001.

[1] [19] Watson P.A., "Slipping in the Window: TCP Reset Attacks", 2003.

First IEEE International Workshop on Critical Infrastructure Protection

The IWCIP 2005 workshop provided a truly international forum for presenting and discussing research in a broad spectrum of critical infrastructure protection and is to be the first in an annual series of workshops.

Dr. Stephen D. Wolthusen

Dr. Wolthusen is associate professor at the Norwegian Information Security Laboratory at Gjøvik University College, Norway and lecturer at the Information Security Group, Department of Mathematics, Royal Holloway, University of London. He also serves as advising senior scientist for the security technology department at Fraunhofer-IGD, Darmstadt, Germany.

The workshop, held on November 3rd and 4th in Darmstadt, Germany, as the first in what is to be a series of interdisciplinary and international workshops on critical infrastructure protection was sponsored by the IEEE Task Force on Information Assurance in co-operation with the *Fachgruppe Kritische Infrastrukturen* (FG KRITIS) of the German *Gesellschaft für Informatik* (GI).

Kindling academic interest

While a number of CIP-related events and workshops had been established over the years, most of these events are characterized by being largely restricted to government and closely related organizations. Academic interest has been scattered with CIP-related research being presented at a number of conferences, but typically only in an isolated fashion.

This has presented academic researchers with a conundrum in that CIP-specific events were typically not refereed and hence were unattractive for publication requirements – while the existing conferences could not provide the depth and breadth of discussion that are an absolute necessity in a field as broad and complex as critical infrastructure protection.

Moreover, the interdisciplinary nature of research in this area necessarily resulted in an even broader scattering of results in the literature.

As a result of this situation and the lack of relevant outlets for discussion and publication, academic research in the CIP area is clearly not as vibrant as it could be. The IWCIP workshop series is in part intended to address this issue by providing a forum for just this research.

The IEEE as an Interdisciplinary Platform

The IEEE provides a reputable and interdisciplinary platform for technology and policy-related aspects of Critical Infrastructure Protection.

The Institute of Electrical and Electronics Engineers is a global organization with more than 350’000 members in 150 countries and covers a broad spectrum of science and engineering through its 38 societies whose field range from the Computer Society through Control Systems, Communications, Power Engineering and Reliability to Nuclear and Plasma Sciences. As such it provides an ideal platform for the similarly broad remit of critical infrastructure protection.

The Computer Society’s Task Force on Information Assurance is the sponsor of the workshop series but is actively engaged in discussions with other IEEE societies to ensure that expertise from all relevant domains is represented.

A stellar program committee

The workshop struck a balance between peer-reviewed papers and presentations on one hand and invited talks on the other hand. Peer review for the research papers was performed by an international program committee of recognized experts in all areas of critical infrastructure protection. This ensured the high quality and relevance of all presentations that was subsequently also reflected in the spirited discussions that were a prominent feature of the workshop. All peer-reviewed papers were published in a conference proceedings volume with IEEE Press.

This ensures broad dissemination of research results since the conference proceedings are also part of the IEEE Digital Library, a resource to which most academic, government, and industry organizations have ready access.

Invited talks from the European Commission and the Bundesamt für Sicherheit in der Informationstechnik

In addition to peer reviewed papers, the workshop also hosted two important invited talks.

Jacques Bus' talk provided important insights into current and future strategies for strengthening European research in the CIP area

In the first invited talk, Jacques Bus (head of the security research unit in the European Commission's IST directorate) provided a perspective on European research and development in the area of resilience for the information infrastructure. In this context, he discussed both the history of European research in the field – particularly as conducted through the EU Framework research programs – and trends towards ever more closely meshed networks of infrastructure elements and the necessary robustness and resilience properties that need to accompany these developments if the reliability and availability of the European Union's critical infrastructures is to be maintained. Dr. Bus then also outlined the anticipated research programs and focal points for funding within the context of the upcoming FP7, outlining a vision of broad research activities.

The second invited talk on IT security in process control by Mr. Hans Honecker of the German Bundesamt für Sicherheit in der Informationstechnik discussed a number of highly relevant problems in the fields of SCADA systems and process control. Here, the conflict between the approaches commonly found in IT security and security architectures and the specific requirements in the SCADA environment were the primary focus; Mr. Honecker also discussed some of the problems arising from the largely safety-oriented culture common in SCADA engineering as it is confronted with an ever more closely interconnected network environment in which assumptions about closed networks are no longer tenable.

Research talks: Day one

The main program of the workshop was organized into six sessions. In the first session on detection and recovery T. Dübendorfer of ETH Zurich (Switzerland) described recent research on worm attack detection and mitigation in the Swiss academic network backbone, while H. Owen of Georgia Tech (USA) presented a local defense mechanism against root kits in the form of a secure microkernel.

Metrics and performance indicators were the focus of the second session. Here, B. Hämmerli of HTA Lucerne (Switzerland) outlined a set of performance metrics that can be used to make the relative security and preparedness of national critical infrastructures transparent and comparable to CIP users such as multinational corporations looking for investment opportunities. U. Maurer of Integralis (Germany) presented a monitoring and surveillance system for critical IT-based processes based on a portal approach.

The third session focused on planning and human factors. J. Barnes of James Madison University (USA) discussed the importance of considering humans as a vital element of any critical infrastructure model and the need to incorporate human interactions whether at the private or public level into all models and reactive systems.

R. Setola of the University of Rome (Italy) analyzed control system strategies for critical infrastructures, arguing for systems capable of introspection and conditional autonomous operation if overall operations cannot be maintained.

The fourth session focused on communication systems; here, J. Eronen of the University of Oulu (Finland) discussed risks identified in a number of protocols that are extremely widespread in critical infrastructures ranging from telecommunications to SCADA environments based on systematic analyses of common elements found in many low-level ICT protocols.

L. Ribeiro of CPqD Telecom (Brazil) then provided an overview of activities and efforts to secure and improve the robustness of critical infrastructures, particularly in the telecommunications sector in Brazil with a perspective to apply the modeling and experience gained in the telecommunications area to other CIP domains.

Research talks: Day two

The second day of the workshop began with a session on civil and power

engineering aspects of critical infrastructure protection. S. Rahman of Virginia Tech (USA) outlined a proposal for increasing the robustness and resilience of electrical power generation while providing increased efficiency at the same time through the use of intelligent and adaptive distributed autonomous power systems.

E. Luiijf of the Clingendael Center for Strategic Studies (The Netherlands) then discussed analyses conducted in the area of civil emergency preparations and the weaknesses uncovered particularly in readiness for larger-scale emergencies and disasters that can have cascading effects. Several case studies illustrated the recommendations by highlighting the need for both preparedness and improved communication cutting across stovepipe areas of concern and jurisdiction.

The sixth and final session of the workshop was started by S. Wolthusen of Gjøvik University College (Norway) discussing modeling and simulation environments for both planning and operational use in command and control systems that are based on geographical information system as the foundation for providing rich contextualized information to decision makers. Such models can be used to both analyze and monitor complex interdependencies among infrastructures while visualization techniques provide decision makers with the ability to obtain insights that are difficult or impossible to derive using automated analytical techniques.

E. Adar of iTcon (Israel) closed the workshop by discussing a framework for risk analysis in the specific context of critical infrastructure protection along with the tools and techniques used to conduct rational risk management in an environment characterized by complex interactions and only limited insight into the overall situation where risk management decisions must be taken based only on partial or limited information.

Workshop Summary

Not only were the authors and speakers of the workshop drawn from the international community, the workshop also hosted participants from close to twenty nations who engaged in open and productive discussions not only in relation to the talks given but also in intensive networking activities taking place throughout the workshop.

Moreover, the roster of participants was almost equally balanced between academic, industry, and governmental participants, fulfilling another important hope of the workshop organizers by bringing these communities together and providing a forum for establishing contacts and future research collaborations.

Further information and materials

The full program of the workshop, along with slide sets (where available, some slide sets could not be declassified) is archived on the workshop series' web site at http://www.iwcip.org/2005; the proceedings volumes can be obtained from IEEE Press or through the IEEE Digital Library.

Current plans call for the next workshop in the series to be held in the Washington D.C. area in the US, presumably also in late October or early November of 2006. The official call for papers will be published in spring of 2006.

The IEEE IWCIP 2006 workshop will be held in the Washington D.C. area

First International IRRIIS Workshop

Evaluation of Existing CIIP Technologies

April 26th, 2006 Fraunhofer Gesellschaft, Sankt Augustin – Bonn, Germany
International workshop with technology providers for Large Complex Critical Infrastructures (LCCI), operators and researchers

Mechthild Stöwer

Consultant and researcher at the Fraunhofer Institute for Secure Information Technology (SIT) Department Secure Processes and Infrastructures (SPI)
Phone +49-2241-14-3123

mechthild.stoewer@sit.fraunhofer.de
http://www.sit.fraunhofer.de

The EU funded Integrated Project "Integrated Risk Reduction of Information-based Infrastructure Systems" (IRRIIS) has started in February 2006. The project aims at substantially enhancing the dependability of Large Complex Critical Infrastructures (LCCI) by introducing appropriate Middleware Improved Technology (MIT) components. In order to understand ICT-related interdependencies of LCCI and validate the functions of MIT components modelling and simulation tools integrated into a synthetic environment are developed as well.

The project is carried out by a well balanced consortium of fifteen partners from research, technology providers and operators of large critical infrastructures.

Focussing on main problem areas of CIIP

The first international IRRIIS workshop will focus on the main problem areas of Critical Information Infrastructure Protection (CIIP). Economic and political, technological and organisational challenges will be identified and evaluated regarding the specific requirements of LCCI stakeholders.

International experts discuss most challenging problem areas and evaluate existing technologies for Critical Information Infrastructure Protection

Inventory of existing technologies for CIIP

Up to now there is a lack of advanced understanding of LCCI dependability and interdependency in particular with regard to the use of Information and Communication Technology (ICT). Although some models and tools dealing with these issues exist, LCCI complexity and criticality cannot yet be tackled properly.

The workshop will evaluate already existing tools and methodologies for CIIP and will specify requirements for the development of simulation environments and Middleware Improved Technology according the specific needs of LCCI stakeholders.

This evaluation and analysis will provide a short- and mid-term vision of outstanding R&D needs.

International Participation

LCCI stakeholders from all over Europe shall participate in this event so as to de-fine their needs and requirements to influence the development process within the project. Since IRRIIS will provide new technologies to support stakeholders in managing the complexity of their interdependent systems and improving their survivability, dependability, and resilience, stakeholders' interests have to be taken into account accordingly right from the project start.

Thus, we would like to invite all interested stakeholders to take an active part and participate in the international workshop. We are looking forward to seeing you at the Fraunhofer Gesellschaft in Sankt Augustin near Bonn.

For more information please see at: http://www.irriis.org (coming soon)

DIMVA 2006

Third GI SIG SIDAR Conference on Detection of Intrusions & Malware, and Vulnerability Assessment
Berlin, Germany, July 13 – 14, 2006

Pavel Laskov

DIMVA'06 General Chair
Tel.: +49-30-63921870
laskov@first.fhg.de

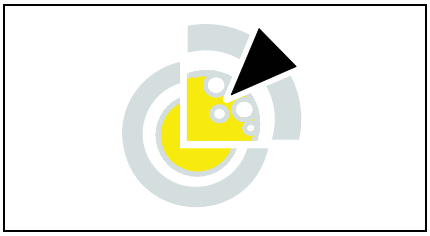
Roland Büschkes

DIMVA'06 Program Chair
Tel.: +49-228-93633485
roland.bueschkes@t-mobile.de

The special interest group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI) organizes DIMVA as an annual conference that brings together experts from throughout and outside of Europe to discuss the state of the art in the areas of intrusion detection, malware detection, and vulnerability assessment. DIMVA is organized in co-operation with the IEEE Task Force on Information Assurance.

Conference Scope

The scope of technical topics is broad and includes, but is not restricted to areas like new exploitation techniques, vulnerability detection, reverse engineering, intrusion detection and event correlation, intrusion response and intrusion prevention, malware detection, malware prevention, as well as computer and network forensics.



The objective of the conference is to give participants an in-depth and focused insight into the current state-of-the-art in research and application. In this spirit DIMVA particularly emphasizes the collaboration and exchange of ideas between industry, academia, law enforcement and government.

Conference Program

The international program committee received more than 40 submissions from 21 countries. Based on the currently ongoing review process for academic papers a two day conference program will be selected by the end of March.

Invited talks will be given by two internationally renowned security experts, namely John McHugh, Dalhousie University, Canada, and Michael Behringer, Cisco Systems, France.

The overall conference program will be completed by short-presentations of selected industry papers as well as a special workshop, which will give Ph.D. students and young researchers an opportunity to present and discuss their current work and recent achievements.

Conference Location

Following the preceding successful DIMVA events, i.e. DIMVA'04 in Dortmund, Germany, and DIMVA'05 in Vienna, Austria, this year's conference will take place at the conference center of Berlin-Brandenburg Academy of Sciences located at Gendarmenmarkt in the heart of Berlin.

Additional Information

For additional background information and updates about DIMVA and SIDAR, please refer to the following sites:

- http://www.dimva.org/dimva2006
- http://gi-fg-sidar.de

We are looking forward to see you in Berlin!

March 28 and 29, 2006, FRENTANI Congress Centre, Rome, Italy
http://ciip.casaccia.enea.it/cnip06
An International great event, with speakers from Complex Network and Infrastructure researchers, stakeholders, emergency management practitioners from across the globe.

Sandro Bologna

CNIP06 International Program Committee Chairman
Phone: +39-06-30483708
bologna@casaccia.enea.it

Claudio Balducelli

CNIP06 General Chairman
Phone: +39-06-30483334

claudio.balducelli@casaccia.enea.it

The goal of CNIP06 International Workshop is to establish synergies between the scientific efforts produced at National, European and trans-European level on the theme of Complex Networks and Infrastructures Protection with particular attention on the new threads, vulnerabilities and applicable defence strategies.

This initiative is sponsored by ENEA, the Italian National Agency for New Technology, Energy and the Environment, and is originated from the proposal to establish a Special Interest Group about this theme on behalf of TIEMS, The International Emergency Management Society.

Addressing different types of networks

Physical networks like electric grids, oil, gas and water distribution networks, transport/road systems.

Cyber-networks like data transmission Internet based, and SCADA, public telecom and Wi-FI networks.

Societal networks like the human teams, organisation, squads and infrastructure costumers that supervise and/or utilise the generated services.

A large spectrum of multi-disciplinary speakers presenting talks from scientific to policy-level perspective, selected by an International Scientific Committee of experts.

Broad International Participation

The workshop benefits from peer-reviewed talks from a truly international roster of speakers with academic, government, and industry speakers from Australia, Belgium, Canada, Croatia, Germany, Israel, Italy, Norway, Poland, Spain, Sweden, Swiss, UK, and USA.

The session themes of the Workshop are: Power Grids, Service Oriented Infrastructures, Structural Vulnerability, Societal Vulnerability, Emergency Management, Dependability, Risk Assessment, Interdependencies, SCADA, Security and Monitoring and Control.

Improved Visibility for C(I)IP

The interdisciplinary character of the CNIP06, together with the fact that it provides a peer-reviewed outlet for research results, should encourage the researchers and the practitioners to work together identifying Complex Networks vulnerabilities and protection needs. The establishment of Interest Groups on such themes and future editions of similar Workshops will be encouraged.

We would like to invite all interested stakeholders to participate in this workshop and hope to see you in Rome.

For more information see:
http://ciip.casaccia.enea.it/cnip06

Selected Links and Events

By the end of February a general link document over all ECN Number will be available on the CIIRCO homepage. Please mail interesting links using the topic "ECN link" to: ***editor@ciip-newsletter.org***

Actual Upcoming CIIP Conferences in Europe

- INFSO D4 events, http://www.cordis.lu/ist/trust-security/events.htm
- IST events, http://europa.eu.int/information_society/newsroom/cf/newsbytheme.cfm?displayType=calendar&tpa_id=7
- From RFID to the "Internet of things", March 6/7, 2006 Brussels, Belgium, http://www.cordis.lu/ist/audiovisual/neweve/e/conf6-70306/conf6-70306.htm See also: Towards a RFID Policy for Europe at: http://europa.eu.int/information_society/policy/rfid/index_en.htm
- Trust in the net, http://www1.eu2006.at/en/Meetings_Calendar/Dates/February/0902TrustintheNet.html
- International Workshop on "Complex Network and Infrastructure Protection"(CNIP'06) March 28-29, 2006 - Rome, Italy: ciip.casaccia.enea.it/cnip06
- 1st CI2RCO Conference on Critical Information Infrastructure Protection, March 30th, 2006, Rome, Italy: http://www.ci2rco.org/events.asp
- International workshop with technology providers for Large Complex Critical Infrastructures (LCCI), operators and researchers, April 26th, 2006 Fraunhofer Gesellschaft, Sankt Augustin – Bonn, Germany: http://www.irriis.org (coming soon)
- DIMVA 2006 - Third GI SIG SIDAR Conference on Detection of Intrusions & Malware, and Vulnerability Assessment July 13-14, 2006 – Berlin, Germany: http://www.dimva.org/dimva2006
- Applied Security Congress and Exhibition September 20&21 2006, Zurich: www.security-zone.info

Conference Papers and Periodic E-Reports

- EAPC / PfP International Workshop on CIP: http://www.dfae.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec.html
- CIP Report USA, is published once a month, accessible with a email note or from the home page: http://cipp.gmu.edu/report
- International Journal of Emergency Management (IJEM): http://www.inderscience.com/browse/callpaper.php?callID=257
- International Journal of Critical Infrastructures (IJCIS): http://www.inderscience.com/browse/index.php?journalID=58#board
- International Journal of Information and Computer Security (IJICS): http://www.inderscience.com/browse/index.php?journalID=151#objectives
- International Journal of Security and Networks (IJSN): http://www.inderscience.com/browse/index.php?journalCODE=ijsn
- Journal of Computer Security http://www.iospress.nl/html/0926227x.php:
- http://www.mitre.org/public/jcs/
- Information Management & Computer Security: http://www.emeraldinsight.com/info/journals/imcs/imcs.htm
- Information Security Technical Report: http://www.compseconline.com/publications/prodinf.htm
- National Security Archive Update, January 26, 2006, http://www.nsarchive.org

Various Resources for IT Risk, Security and Disaster Management

(by Prof. Urs E. Gattiker, ***WebUrs@WebUrb.dk*** *)*

- IT security and various resources (home, SME) (http://del.icio.us/WebUrs -- this list of links is regularly updated and expanded upon – with RSS feed (http://del.icio.us/rss/WebUrs) for being kept abreast about new content and changes
- Various resources to protect home PCs and help SMEs – this list of links is regularly updated and expanded upon – with RSS feed (http://www.listible.com/feed/list/best-pc-security-sources) for being kept posted about new content and changes
- It risk management and disaster recovery resources –this list of links is regularly updated list and expanded upon – with RSS feed (http://www.listible.com/feed/list/best-it-risk-management-sources) for being kept posted about new content and changes
- Alerts, tips, tricks and EU-IST news (http://casescontact.org/) -- provides alerts either via RSS feed (http://CASEScontact.org/rss.php or also with subscription to e-mail newsletter (http://casescontact.org/subscribe.php)