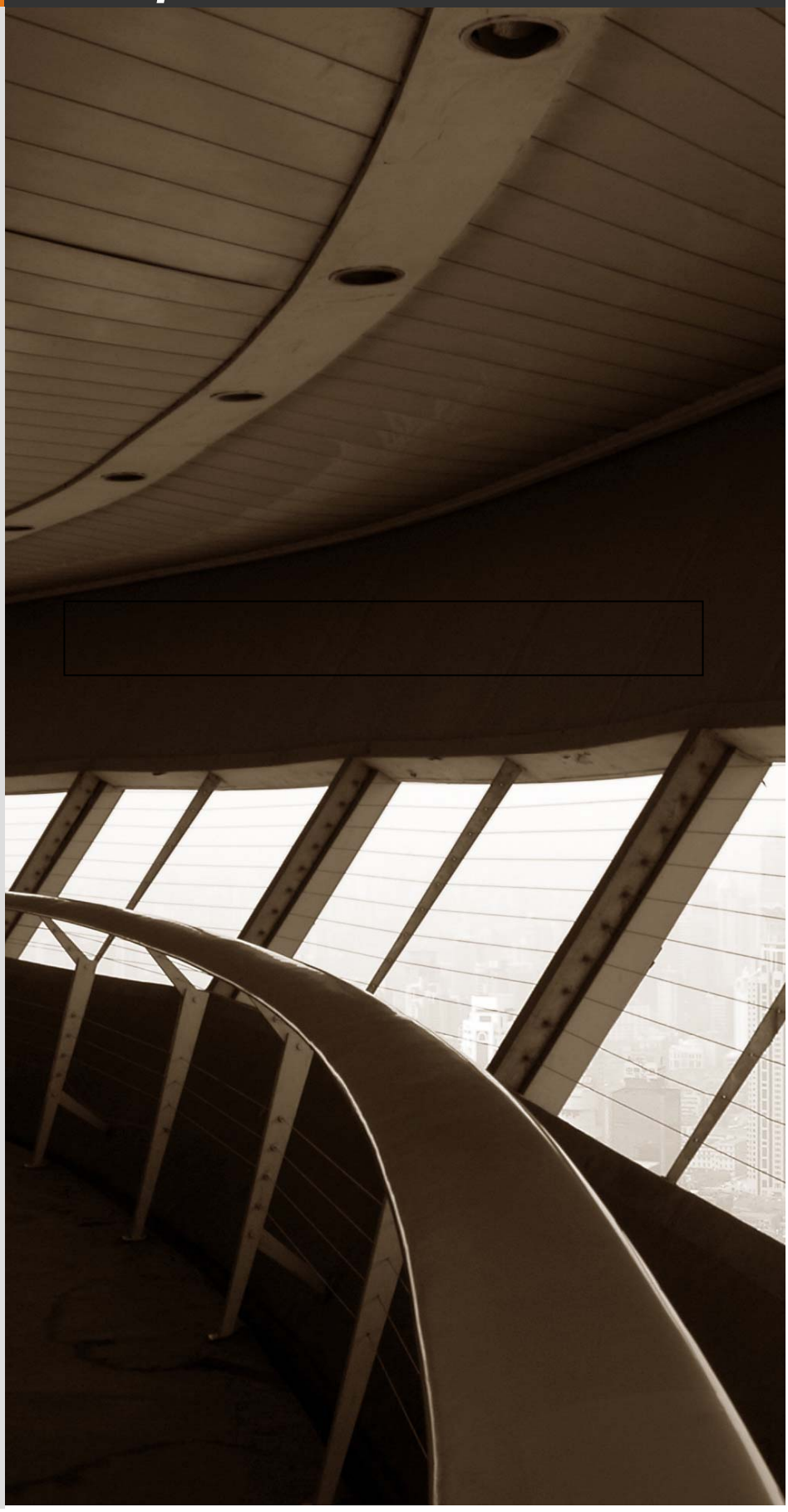
April / May 2009, Volume 5, Number 1

ECN

European CIIP Newsletter



IRRIIS

> About ECN

ECN is co-ordinated with
The European Commission, was initiated by Dr. Andrea Servida,
and is now coached and supervised by Angelo Marino.
For 2007-2009, the ECN is financed by the IRRIIS project.
The IRRIIS project is an IST FP6 IP,
funded by the European Commission
under contract no 027568

>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 site for specific issues:
http://irriis.org
http://www.ci2rco.org

>Founders and Editors
Eyal Adar CEO iTcon, ***eyal@itcon-ltd.com***
Bernhard M. Hämmerli, HTA, Initiator and Main Editor ***bmhaemmerli@acris.ch***
Eric Luiijf, TNO Defence, Security and Safety, ***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***
For Spain: Javier Lopez, UMA, ***jlm@lcc.uma.es***
For Finland: Hannu Kari, HUT, ***kari@tcs.hut.fi***

> Spelling:
British English is used except for US contributions

Table of Content

Introduction

European Activities

Special Focus: C(I)IP In Finance: CFI

News and Miscellaneous

Selected Links and Events

C(I)IP goes Finance

The European Commission has started the Coordination Action Parsifal as well as another Specific Targeted Research Project (CFI). But what are differences associated to CFI?

Bernhard M. Hämmerli
Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
Vice-President ISSS Information Security Society Switzerland and Chair of Scientific and International Affairs

e-mail: bmhaemmerli@acris.ch
bmhaemmerli@hslu.ch

Uniqueness of CFI

It is a well recognised fact that Critical Infrastructures (CI) comprise a set of sectors, with slight differences per nation. But is there a need to research each sector separately in respect to security and CIP – or is just any sector alike the others? Debating on these issues specifically for CFI, the following outcomes were elaborated

Reputation Risk and Trust

Maintaining the near "zero fault tolerance" of the financial sector while driving costs down. CFI faces enormous reputation risk because trust is the fundamental value of the financial sector businesses. Therefore, even for post incident measures and preparedness, huge investments are made.

Transparency and Density of Policies and Regulations

Policies and regulations are changing over time and force the financial sector to provide great transparency on all aspects: from real time monitoring to 50 years of archiving, each single action in a traceable and non repudiation way. Even as the health sector has many regulations; its requirements for the ICT-infrastructure is not comparable to those for the financial sector.

Combination of Complexity and Security Properties

The complex logistics of management issues in the security topic (keys, identities, entitlements, etc.), especially for the effort of one common and liberalised European finance market, are a new and unique challenge for technology but also for the evolvement of the business model. The combination with security requirements for simultaneously maintaining high availability, integrity, the highest confidentiality amongst all sectors and **real time quality** is very unique. The financial sector is extremely interconnected, nationally and internationally and no other sector is using so many real-time interconnections transporting so much money on it.

Changing Business Models and Technology

The missing strategic security awareness and preparedness for next generation technologies and emerging and changing business models are shared by many stakeholders in the financial sector. E.g. plastic cards will dematerialise to electronic entities in cell phones, new players entries such as eBay, Amazon, Google arise.

Unique Position within the CI Application Sectors

Many CIP models are structured such that electricity and telecommunications are base infrastructure services. Most critical sectors and/or services operate on top of them. No other application sector is so much interconnected with any other sector as the financial sector: Therefore, the dependability of society of the financial sector is so large that during the recent financial crisis, more support by governments was given to the sector than to any other project in history.

Conclusions: The enumerated uniqueness needs well tuned research efforts directed to financial applications and its expectancies, even if the basic security concepts do not substantially differ from other sectors.

About this Issue

Angelo Marino and Thomas Skordas, both from DG Information Society and Media Unit 1.4 write on EU research in critical infrastructure protection (CIP) and give an overview of the various EU research activities in the CIP area. They

share their views on some additional activities needed for research and innovation support and for technology transfer.

Randel Crowcher, former Security Officer of the Royal Bank of Scotland asks himself the question: "Identity: the new critical information infrastructure?" On the base of growing number of 'perimeter less' environments, he states that the ability to establish and validate identity and entitlement is critical, and becoming ever more complex.

Matt Broda, Senior Security Strategist for Microsoft's CIP Program and currently responsible for the globally expanding program, shares his experience on Cyber Security and the "Five Lessons Learned". The lessons address the situation with evolving threats and new technologies present growing risk for Critical Information Infrastructures around the world. The identified lessons are a kind of industry good practices for CIP.

Semir Daskapan and Julien Ubnacht from Delft University, The Netherlands developed an approach to increase dependability in complex adaptive systems: the complexity of critical information infrastructures can be exploited to improve their dependability when they are designed according to a complex adaptive systems method. Policy makers should select an adequate governance approach and stimulate infrastructure providers to adopt the CAS-Approach.

César Pérez-Chirinos, Professor and Business Continuity Unit Manager in Banco de España, writes on, operator security plans (OSP) and Business Continuity Plans (BCP) in financial institutions which are considered to be a critical infrastructure. He gives an overview on good practices in software engineering and test driven development TDD. He inter-relates it to good practices for BCP writing at CFIs and looks at compliance with the EPCIP Directive requiring Operator Security Plans (OSP) including BCP.

Eric Luiijf, Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands, writes on SCADA Systems using the well thought title "Are you in Control?" He reports on the second Dutch Process Control Security Event at the Technical University of Delft, December 4, 2008 and gives an overview of the key questions discussed.

The CRITIS conference Series will continue with the 4th International Workshop on Critical Information Infrastructures Security in Bonn St. Augustin, Germany, Sept. 29-Oct 2, 2009 http://www.critis09.org. A resume of the last conference CRITIS'08, 13th to 15th of October 2008 in Rome is given. This should make the readers keen to attend this years' conference.

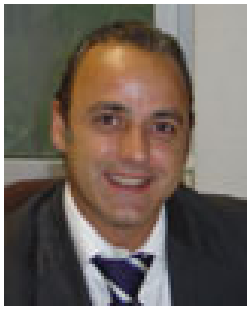
As always, selected links – mostly derived from the author's articles – and events conclude this issue.

Enjoy reading this issue of the ECN!

PS. *Authors willing to contribute to future ECN issues are very welcome. Please contact me or one of the national representatives. Further information about the ECN and its publication policies can be found in the introduction of the first ECN, see* www.irriis.eu.

EU research in critical infrastructure protection – CIP

In this article, the authors provide an overview about the various EU research activities in the field of Critical Infrastructure Protection (CIP). They also provide their views on some additional activities needed for research and innovation support and for technology transfer.



Angelo Marino

Project Officer
DG INFSO Unit "Trust and Security"
e-mail:
Angelo.MARINO@ec.europa.eu

Thomas Skordas

Deputy Head of Unit
DG INFSO Unit "Trust and Security"
e-mail:
Thomas.Skordas@ec.europa.eu

Critical Infrastructures (CIs) of our modern societies heavily rely on information and communication technologies (ICT). ICT is rendering them more intelligent and globally interconnected but also more complex and dependent, more difficult to manage and control, and therefore more vulnerable.

Several incidents and disruptions have demonstrated current technology limitations to manage highly complex CIs efficiently and to protect them against attacks orchestrated via the cyberspace. Cross-sector and cross-border dependencies on ICT infrastructures can provoke cascading effects, caused by dependencies and interdependencies across different interconnected CIs and their services. Therefore, present and future CIs must be able to tolerate anticipated high levels of threat and still perform in a trustworthy manner.

Given the above, in the last few years the EU as well other regions of the world have launched a set of complementary policy and research activities aiming at substantially improving the protection of CIs.

On the policy side: In 2006, a European policy package on the protection of CIs (EPCIP) was adopted by the European Commission for the period 2007-13. The package comprises a communication dealing with general policy linked to EPCIP and a directive focusing on the identification and designation of pan-European Critical Infrastructures (see http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm). The directive has been formally approved at the end of 2008 and the Critical Infrastructure Warning Information Network (CIWIN), part of EPCIP, should be operational within 2009. Following a sector specific and all-hazard approach of the directive, the identified specific CI sectors are in the process of defining the criteria for the identification and designation of European Critical Infrastructure (ECI). In ICT in particular, a specific policy initiative on Critical communication and Information Infrastructures Protection (CIIP) is planned for the first half of 2009 with the objective to enhance the level of CIIP preparedness and response across the EU.

At the research side: To take account of the multiple dimensions of security-related threats to Europe, one of the eleven working groups of ESRIF (European Security Research & Innovation Forum) is focused on the security of CIs. An intermediate status report was presented at the 3rd European Security Research Conference SRC'08 that was hosted by the French EU Presidency on 29-30 September 2008 in Paris. ESRIF is expected to deliver its final recommendations in autumn of 2009 (http://www.esrif.eu/index.html).
The main stakeholders operating in the field acknowledge that there is significant deficiency in theoretical understanding of phenomena related to CIP. As part of the response, system, organisational and business resilience seem to emerge as a new paradigm that is under discussion by the key stakeholders involved in the protection of CIs. However, many issues relating to the realisation of this paradigm remain open today, including technology and systems development aspects, which require new research efforts for addressing them.

It is in this context that European Commission ICT research efforts on the protection of CIs and more specifically

on resilient and dependable CI's are to be seen. Our research efforts started in 2004, with the funding of about nine projects in the field under the IST-FP6 programme. Projects like IRRIIS, CRUTIAL or DESEREC address the development of new technologies aimed at limiting failure consequences and at improving the overall resiliency of CIs. The GRID and CI^{2}RCO coordination actions brought together the main research stakeholders in the field, matched national and regional research programmes and focused on defining new promising research directions for the constituency to address in the next few years. For more details on these projects, see at http://cordis.europa.eu/ist/trust-security/projects.htm.

The latest (2008) FP7 research initiative on the protection of CIs is a joint effort between the FP7 ICT and Security Programmes (see respectively: http://cordis.europa.eu/fp7/ict/ and http://ec.europa.eu/enterprise/security/index_en.htm). The initiative aimed at providing a concrete platform for the stakeholders to explore, create and evaluate new multi-disciplinary technical solutions in developing resilient CIs, thereby researching both specific ICT solutions (under the ICT Programme) and their integration into larger protection systems (under the FP7 Security Programme).

As a result, nine new projects are about to start under the ICT Programme with the following objectives:

- Developing knowledge and technologies for understanding and managing the interactions and complexity of interdependent CIs).
- Building secure and resilient networked information and process control systems operating in CIs; improving the capacity of assessing risks, facing contingency and dynamically reacting to failures of CIs.

In more detail, each of these nine R&D projects is addressing the following main lines (the amounts below indicate the EC funding):

- **MICIE** (2.5 years, 2.5m€): A real-time alert system supporting the decision making of CI operators that predicts risk from threats and the likely cascading effects that may emerge;
- **PEACE** (27 months, 2.65m€): An emergency management framework for next generation all-IP networks ensuring secure multimedia communication in extreme emergency situations;
- **SERSCIS** (3 years, 2m€): A methodology integrating modelling and management of CIs through adaptive Service Oriented Architectures;
- **WSAN4CIP** (3 years, 2.7m€): Secure and fault-tolerant wireless sensor and actuator networks for use in the protection and management of CIs;
- **INSPIRE** (2 years, 2.4m€): Secure configuration and management of communication networks in distributed control systems operating in CIs;
- **VIKING** (3 years, 1.8m€): Improving the robustness and security of industrial control systems operating in electric power networks;
- **UAN** (3 years, 2.95m€): Developing a security-oriented underwater wireless network infrastructure for the protection of off-shore plants;
- **COMIFIN** (2.5 years, 2.35m€): Protecting financial infrastructures against operational failures and cyber threats by using a secure scalable overlay communication middleware;
- **PARSIFAL** (1.5 years, 0.6m€): A coordination action bringing together ICT security and financial stakeholders for identifying best practices and new research priorities in protecting financial CIs.

Further technical details on all the above projects can be found at the following web site: http://cordis.europa.eu/fp7/ict/critinfpro/projects_en.html. In addition, the **DIESIS** project (http://www.diesis-project.eu/) aims at establishing the basis for a European modelling and simulation e-Infrastructure to foster and support research on all aspects of CIs.

While these projects will help moving ahead the EU's research agenda on CIP, complementary and well coordinated activities for research and innovation support and technology transfer would also be required from the CIP research constituency, in particular:

- Agreeing frameworks, platforms and tools for data collection and trusted data sharing on incidents and vulnerabilities as well as on countermeasures in CIs; these would enable researchers to work with fresh and contextual data and address the real issues at stake;
- Defining agreed security metrics, and developing benchmarking and testing facilities that are openly accessible by the stakeholders and sustainable in time; this includes test beds for CIP technology assessment, awareness raising and confidence building.
- Agreeing upon best practices and upon certification and standardisation;
- Developing mechanisms for attracting and involving CI stakeholders with 'on the terrain' experience, in particular TSOs (Transmission Systems Operators).

The above are some of the issues in EU's agenda for the coming years.

Disclaimer: The views expressed in this paper are the sole responsibility of the authors and in no way represent the views of the European Commission or its services.

Identity: the new critical information infrastructure?

In the growing number of 'perimeter less' environments, the ability to establish and validate identity and entitlement is critical, and becoming ever more complex.

Randle Cowcher

Director and Managing Consultant, Aicoute Consulting Ltd., leading in provision of practical security and entitlement solutions for financial, civil and military organisations.

e-mail: randle.cowcher@aicoute.com

What happens when the lights go out? Not just for a short period, but when it may take weeks or months to re-establish a reliable mains electrical network. We now take for granted that our various local, national and international networks for services and commerce will only suffer very short interruptions. When a credit card is not accepted at the end of a purchasing process, it is a major frustration whether it's the person at the front of the line forgetting a PIN or if the entire credit network has failed. In all cases credentials need to be re-established, whether personal, the store, network node or the host connections. Establishing the correct user identity and their entitlement(s) is vital.

"One-in-a-thousand-year events seem to be happening annually, and one in a hundred year events are occurring weekly at the moment. All our risk models need to be reviewed, updated and re-applied"
Lord Turner, February 2009

How do you prove your identity and entitlement when the mainstream systems have failed?

In modern times, it typically takes decades for a new infrastructure to become established and 'trusted'. Some newer services, such as mobile phones, have rolled out more quickly but most of our energy, transport, supplies and commerce infrastructures have taken more than 50 years to reach the point of being taken for granted. Each has a complex set of credentials, processes, passes and tests before one can gain access. Getting an energy user account number, a permit to drive and park a vehicle, or access to an aircraft as passenger, freight or crew requires increasingly complex forms and networks for identity.

The drive for instant gratification is creating new vulnerabilities - from the databases to the end user terminals

Financial Services have been at the forefront of organised identification from before the Middle Ages; the network of traders, money lenders and feudal landlords may not have met and know each other on sight, but had established identity marks, signatures and codes that enabled robust recognition. If you wanted to set up a business or services in a new area, a 'letter of introduction' was often required, and the supply of such letters soon became a business for the banks, where local knowledge about you could be summarised in short codes that would be recognised by similar organisations. For national representatives, a system of 'passports' became established, and spread down to ever wider levels of citizens. Now we have a number of 'standard' forms of identity including passports and national identity cards, credit and debit card accounts, social security and national health numbers. But these 'standards' are rapidly becoming degraded in value as system after system sustains massive data losses, 'hacks' and the revelation of tools and techniques to discover, copy and take over, or even predict and create false identities.

Even the 'secure' networks begin to look compromised…

Recent revelations question the security and integrity of some of the switches that lie at the heart of our national and international data and voice networks. If these can be compromised or accessed covertly without the appropriate authority, enormous damage may occur from outright denial of service to miss-routing, illicit duplication and enabling such access to sensitive information so that all trust by users is undermined. Of course some government and corporate networks have been designed specifically to minimise such risks, but the high financial and operational costs make their continued use, in the face of ever greater commercial and user pressures, one that may be difficult to sustain.

There are good commercial and operational reasons for the new or emerging networks and infrastructures such as 'Cloud Computing'; satellite-based networks with broad and narrow-cast services; merged mobile, internet and corporate networks. User demands for instant availability and access to all data sources and services are forcing a simplified and common approach – so called "convergence". The user's portable terminal (mobile phone, PDA, micro-computer, e-reader etc.) does not have the space, power and capacity to handle lots of different authentication, encryption, digital rights management and other such security and integrity tools as overheads to already much-compressed data streams. The networks and database systems are designed to push data out as quickly and in as common a form as possible, rather than questioning the rights to access. Passwords are hidden, hard-coded, minimised or ignored in the rush to gain speedy access. So the balance of security and access is tipping towards ease of use, simplifying and minimising the overheads that would otherwise maintain separation and security, so creating a huge looming future vulnerability.

However, it is not just at the user terminal that a simplified security structure is emerging. For at least two thousand years man has been building and using massive databases. Until very recently access to these national and corporate databases was highly restricted, complex and required arcane knowledge of protocols and processes to conduct searches. The transmission of information between such databases was tightly controlled and mainly restricted by the limitations of any technology to allow such transfers. But all this has changed with the new data networks and common standards such as the internet protocols. Now we have enormously powerful search tools and 'engines' that can readily and rapidly access, inspect, retrieve, translate and present complex searches of numerous databases and sources in fractions of a second.

At the same time, there has been an international shift in culture allowing or mandating that so much more information must be made readily accessible and available. "Freedom of Information" legislation backs up demands from users of all types for open, or near open access to most information. The young, and less security aware, willingly provide astonishing details of their personal lives, likes, pets, habits and family, as well as their contact details, copies of signatures, photographs and other biometrics. While corporate users historically understood the reasons for protecting information held in secure data centres, private individuals seem to demand public access to their data, and the resulting issue that the public gains access, rather than just themselves, seems to be forgotten.

All this information is openly available via the numerous and burgeoning social networks such as Facebook, MySpace, BeBo and LinkedIn. It is compounded by willingness for governments and their agencies and many corporations to give access to their numerous databases. Schools publish their records, local authorities allow access to civic records and the records of data and library or open medical searches can be inspected to indicate all sorts of personal and medical data, even including DNA profile information. There are readily available databases with the family details of millions of citizens, making the discovery of a 'mother's maiden name' or social security number very easy. Now we are beginning to see the emergence of profiling programmes (e.g. Spoke, phorm etc) that automatically search and collate all this information, ready for download and misuse.

"Incidents of data loss have become a worryingly regular occurrence. Now, on hearing that many databases are poorly managed, fundamentally flawed and even potentially illegal, the public has every reason to fear for the security of their personal information." **Chris Mayers, chief security architect at Citrix – March 2009.**

Thus we are creating and reinforcing ever faster infrastructures for our own downfall; the criminal is heading to a position where they know, and can readily prove more about you than you can yourself!

We also need to consider the environments in which our security policies reside. We have become very much better at writing comprehensive security policies for our organisations, but rarely think either how they will be interpreted or understood by the users, or how they will interact with the 'real-world' environment, let alone the infrastructures feeding to and from that organisation. There is currently a panicky move by governments and corporations of all sizes to hugely restrict the ability of staff to copy or transmit data, through the removal of access to all USB ports, and deletion of ability to copy to removable disks of all types and a general 'locking-down' of

the work environment. At the same time, encryption is being introduced 'en masse' with little thought to the medium or long term consequences. As a result, staff, contractors and visitors are rebelling and finding simple ways round these blanket restrictions in ever more devious ways. The worst exponents are normally the most senior staff, but they know that information still needs to be communicated to meet deadlines or to keep the business going. Information Security, previously a non-functional requirement needs to be recognised as a basic function of the systems. The result of this restriction is that information that would normally have been encrypted, loaded to disks and couriered is being sent in clear in the body content or as attachments to open e-mails. This is particularly prevalent for managers wishing to work on projects and documents at home or in remote offices. As they are no longer allowed to load such information to memory sticks, they send it without realising how much of a compromise this is to the longer term security of their organisations, as it creates opportunities for the properly encrypted files to be 'broken' and accessed. If the normal data links are overly restricted, it becomes increasingly tempting to simply use a fixed or mobile phone to pass the information.

More than half of savers would move their money if their provider lost personal customer details.
Ipsos MORI- March 2009.

So what does this all have to do with Identity and Entitlement?

Why should these factors be critical and affect our critical information infrastructures, and more importantly, what can we do about it?

As we are all increasingly recognising, most of us have several necessary identities, each of which requires appropriate levels of security and integrity. As a simple citizen the requirements may be very basic, but as soon as your medical information, age – related or local entitlements come into play (such as student accesses, entitlement to concessionary transport or other social services) the value of identity escalates. Financial services typically recognise the need for at least three levels of identification: As a general customer (e.g. to promulgate interest rates); as a specific customer (e.g. to provide account balance information); as a validated account holder (e.g. to allow the set up of payees and the payment or transfer to existing and new accounts). When you then add in the numerous roles that occur in the working environment, including customer, signatory, authoriser, guarantor etc. then the situation becomes very complex. For some of these roles, there is a valid expectation of anonymity; the organisation receiving such a request should not need to know exactly who is asking to provide the requested information. For other roles, it is important that both the customer and the organisation know exactly who (and in what role) they are talking to.

There are fine nuances and implications in establishing and communicating with each of these identities. In the regulated environments, certain levels and techniques for the validation of identity are expected or mandated. Increasingly this requires much more than the supply of a simple stated user identity; complex password exchanges, two and three factor authenticators, and now all sorts of biometrics including face, iris, fingerprint, voice, electrical and chemical property recognition systems come into play. As this all becomes more complex, so does the risk from failure; not just by the relevant system, but also by the user and the technology they are meant to be using *and* the organisation that issues the identity credentials and validators.

The operators of most large-scale databases reluctantly admit that they have a significant problem with "data cleansing"; the duplication and errors that occur over time are rampant in even the most carefully managed database, and can often approach 50% of all data entries. National databases, such as for citizen registration and national identity, health, vehicle management, local authorities, energy services and utilities, work and pensions have all proved to be some of the worst offenders. Yet these are the very databases upon which we most rely for the valid establishment and propagation of 'authorised' identity. Every time there is an interruption of these services, or the systems and updates that feed into them, the problems multiply.

So back to the lights going out: as each minute passes, the master databases progressively go out of synchronisation, even if they have been kept going by 'uninterruptable' power supplies. The value and reliability of the data held decreases. Despite the numerous worthy studies that have been and are currently underway in the EU and elsewhere, looking at critical infrastructures, very few of them take on and rate the inter-dependencies between the energy, utilities, transport, communications, government and finance infrastructures. There may be power, but no transport prevents operators from getting to work; there may be food, but is it accessible in the places it is required? Data may be maintained, but the world around it may be changing and thus degrading it.

As we are talking about critical infrastructures, security and integrity are as important as availability. But to maintain security and integrity, we need to establish the identity of all staff, customers, contractors etc. For staff with pre-issued credentials, such as staff identity cards, licenses and passports, this can work for a while by manual inspection. For remote and on-line services, it all begins to fall apart quite quickly if the links needed to validate credentials cease to work or be reliable. An interesting, if tragic, example of where the systems broke very quickly is the 26 December 2004 Indian Ocean tsunami, resulting in urgent requests from thousands of well meaning or

validly concerned individuals and officials from over 120 countries inundating the authorities and services of the directly concerned nations. All forms of communications (that still worked) were swamped with valid and invalid demands and details. Even long after order was restored, the demands for DNA profiles, fingerprints and other descriptions, details of passports, ID, credit and debit cards were widely circulated to open sources with little or no validation of the sender or recipients. This provided an enormous amount of free data for the criminal, malicious and simply mischievous that still affects us years later.

New "chains of trust" are required…

In such circumstances, we need to quickly re-establish "chains of trust" that can be validated at every stage, and hold good only for a defined period. The technologies that can cope with millions or billions of identities in a provably unique and secure manner have been with us since the mid 1970's, and are being increasingly utilised by the financial services industries (e.g. Swift and many of the payroll and money transmission networks); by major corporates (for product tracking and validity checking); and by national authorities for transport, entitlement and identity services. But in the main, these are centrally imposed functions, and if the communications with the central issuing service fail, so does the system. There are many ways in which the identity services can be distributed, and function when many of the links in the (secure) network cease to work, but to date, there is little evidence that these techniques are being adopted currently.

The value of identity must be properly recognised and its crucial role in the establishment, access, use and development of virtually all our critical infrastructures needs to be studied further and appreciated more. The testing and 'stress models' that are required to validate and accept such infrastructures need to be updated and to take into account the inter-relationships that appear to have been missed in the current versions.

Contributory assistance from the following is appreciated:

Professor Peter Guthrie OBE, FREng
Centre for Sustainable Development
Department of Engineering
University of Cambridge, England.

Adrian Seccombe
CISO and Senior Enterprise Information Architect, Eli Lilly and Jericho Forum member.

Peter Dalziel MBA BSc CMgr
Director, Aicoute Consulting Ltd.

Cyber Security: Five Lessons Learned

Evolving threats and new technologies present growing risk for Critical Information Infrastructures around the world. This article explores some of the industry best practices for protecting them.

Matt Broda

Matt Broda is Senior Security Strategist for Microsoft's Critical Infrastructure Protection Program currently responsible for expanding program's reach globally.

E-mail: matt.broda@microsoft.com

In just over 10 years the Internet and the World Wide Web have revolutionised the way people live. We communicate differently (think Skype, Instant Messaging, Facebook), work differently (consider remote collaboration, video conferencing, Wikis and central document repositories), and do business differently (look at e-commerce, eBay, and on-line banking). But at the same time these innovations have introduced a new type of crime.

The rapid growth of our reliance on cyber infrastructure and services has created vast opportunities not only for individuals, businesses, and nations, but also for criminals and organisations with malicious intent around the world. The pace of technological advancement inevitably left key issues to be addressed later. Best practices for resilient system design and cyber security are examples of areas that have been struggling to catch up with the evolving threats in the recent years.

As cyber space grew and evolved it became increasingly indispensable to many other sectors of economy and critical infrastructure. It is now an integral element in sectors such as banking, energy generation and delivery, health care, and transportation, which make bulk of critical infrastructure across the globe.

Microsoft, with its broad market success became a big target for cyber attacks at the turn of the century, culminating in the early 2000s. This prompted the company to establish its Trustworthy Computing imitative to systemically improve the resiliency and security of its products and solutions. In recent years these efforts have brought measurable results:

- Windows Vista® during its first year in market reduced vulnerabilities by 45% compared to Windows XP in its first year; there were only nine patch events during this period in Windows Vista compared to 26 in Windows XP; as of April 2009 the infection rate of Windows Vista SP1 is 60.6% less than that of Windows XP SP3
- Internet Explorer® 7.0 during its first year reduced vulnerabilities by 53% compared to Internet Explorer 6.0
- SQL Server® 2005 reported no vulnerabilities during its first year

The focus of this article is to introduce the lessons learned in the process of making security part of Microsoft's DNA. At the same time, the themes discussed below are relevant to current European focus on Critical Information Infrastructure Protection.

Lesson 1: Commit to Excellence

Without decisive top-level commitment a cyber security programme is unlikely to reach its maximum potential. The need for improving the protection of critical information infrastructure at national and enterprise level needs to be recognised by the leadership and a commitment needs to be made to support a long-term programme.

There are several key success factors common to the organisations that do it right:

- Establish clear accountability for the programme and ensure that the accountable leader has full support in executing the programme
- Ensure that the programme is funded and resourced for success
- Communicate broadly ensuring that every affected individual participates and contributes – drive awareness, education, and training
- Don't stop when the immediate programme goals are achieved – commit to continuous improvement and invest in ongoing innovation to keep up with evolving threats

Microsoft's journey began with Bill Gates, then Chairman and Chief Software Architect, making Trustworthy Computing the company's top priority in 2001. This long-term, top-level commitment has resulted in building a strong organisation focused on continuously working with Microsoft Research and Development to understand the threat environment, ensuring a high level of software assurance, and to develop new and innovative ways of improving trustworthiness of Microsoft products.

Lesson 2: Ensure out-of-the-box Security

To be effective, security needs to be an integral part of the solution throughout its lifecycle. Although incremental improvements can be accomplished with a bolt-on security approach, their effectiveness is limited and they often become a burden on the organisation in the long run.

The most effective – as well as usually the least costly, approach to cyber security starts at the concept or design stage and follows the product or solution development process. Security needs are met at every step according to the level dictated by the expected magnitude of threat and the ultimate value provided by the solution.

At the same time it is important to recognise that with many modern technologies the people that use or operate them are the weakest link in the security chain. To address this, the technology must require the minimum amount of configuration to achieve the highest possible level of security. Furthermore, the security mechanisms must be user friendly and enable productivity rather than impede it.

Finally, any solution will need ongoing maintenance, updates, and patches. Security vulnerabilities are a fact of life – they need to be dealt with when they are discovered in an effective and timely manner that meets the needs of the researchers, vendors, and end users. A process must be in place to accomplish this for any deployed computer system or network.

Microsoft has embraced all these elements in its SD3 philosophy (Secure by Design, Secure by Default, Secure in Deployment) combined with the Security Development Lifecycle process that underlies development of all Microsoft's key products. The key tenets of this methodology are gaining adoption outside of Microsoft as well.

Lesson 3: Manage Operational Risk

No two deployed solutions are identical. Every system operates in a slightly different environment and is exposed to somewhat different threat vectors. This makes risk management for information systems an indispensable art.

To begin with, assessing the risk in information infrastructure requires a different approach than those used for physical assets. Given the highly distributed, interdependent and often virtualised nature of IT solutions, a function-based, top-down approach most often works best.

The assessment should begin by understanding the critical functions and services provided by the information infrastructure in support of critical assets and services in the physical world. Once these are identified, a combination of threat modelling and threat scenario approaches[1] is used to identify and prioritise the risks that need to be managed.

In addition to understanding the risks affecting the critical functions of the information infrastructure, it is also important to understand the interdependencies among these functions and with the external environment. This is especially important when dealing with national cross-sector information infrastructures or international scenarios. The goal is to identify and manage possible cascading failures.

Microsoft has been very successful in using many elements of the risk assessment methodology, including threat modelling and threat scenarios, and has published tools to enable others to adapt these best practices. At the same time Microsoft worked with the broader industry to build a risk assessment framework designed specifically for Critical Information Infrastructures.

Lesson 4: Enable Resilient Deployment

Ultimately, as with any type of Critical Infrastructure, resiliency is the key goal for Critical Information Infrastructures. Resiliency builds on top of strong top-down commitment, out-of-the-box secure technology and effective operational risk management. It requires alignment of policies, people, processes, and technology.

[1] The **threat modeling approach** begins with identifying the significant consequences that need to be guarded against and identifying the combinations of threats and vulnerabilities that could lead to them. The **threat scenario approach** on the other hand begins with a specific threat and vulnerability and leads to identification of consequences these are likely to lead to.

- The technology needs to embrace cyber security principles at every level – from individual software component to entire network segments – resulting in a comprehensive defence in depth solution.
- The process must support effective operational response and recovery. It must also ensure ongoing system maintenance including vulnerability management and patching.
- The policies must be consistent with the security objectives and enforced in a disciplined manner. They must support trusted information sharing between interdependent infrastructure operators to enable coordinated response.
- The people must have sufficient understanding of the technology, policies, and processes to be able to effectively manage the risk and respond in disaster scenarios.

Building resilient information infrastructure requires continuous testing and tuning of the elements. This is best done through different types of exercises – from discussion-type exercises to operations-based exercises. Microsoft has been involved in running many such exercises (including the CyberStorm series) and has developed tools and training to assist others.

Lesson 5: Raise the Bar across the Ecosystem

Finally, in today's critical infrastructure no company is an island. The ICT sector is characterised by a complex and highly interdependent supply chain. The security and resiliency of the deployed Critical Information Infrastructures ultimately depends on the aggregate capabilities of the entire supply chain.

Taking as an example telecommunication or finance infrastructures, they consist of thousands of components, both hardware and software, manufactured by hundreds of different vendors from around the world. The only way to improve the resilience of the CIIs is for the key stakeholders to raise the bar by working with their suppliers and through education, sharing tools and best practices, and setting incentives and common requirements.

The attackers will likely target the weakest link in the system. Microsoft's Security Intelligence Report version 6[2] clearly shows this trend: as operating systems become more secure the attacks move up in the stack and focus on the less secure applications (nearly 90% of disclosed vulnerabilities affected applications). To address this growing problem Microsoft is active in several key initiatives focused on improving the security across the whole ecosystem:

- The End-to-End Trust[3] vision announced by Scott Charney at the 2008 RSA is a growing ecosystem programme with the goal to establish a trusted stack across hardware, software, people and data creating an environment when exploiting vulnerabilities will become very difficult
- SAFECode[4] (Software Assurance Forum for Excellence in Code) brings together software industry leaders to join forces in defining and disseminating best practices in secure software engineering
- ICASI[5] (Industry Consortium for the Advancement of Security on the Internet) is a forum created by leading global IT vendors with a focus on driving excellence and innovation in security response

[2] http://www.microsoft.com/presspass/newsroom/security/factsheets/04-08SIRv6FS.mspx
[3] http://www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx
[4] http://www.safecode.org/
[5] http://www.icasi.org/

Looking into the Future

As the evolution of ICT continues and even accelerates we can be certain that new cyber security challenges will emerge. Cloud computing promises to bring significant cost of ownership savings, faster development cycles for new services, and improved business continuity; at the same time the technical solutions must address user concerns around the safety and privacy of their data. Deperimeterisation and proliferation of mobile computing enables new business models but at the same time creates challenges for the legacy security systems still relying on perimeter controls. The vision of a trusted on-line environment seems to be the final frontier in cyberspace.

At the same time the practices discussed here continue to provide a framework for a comprehensive cyber security approach:

- Cyber security requires a commitment regardless of whether the solution is in a box or in the cloud
- Security needs to be designed into the solution from the start and maintained through its lifecycle
- Resiliency requires a broad systemic approach and cooperation across the supply chain

When supported by an effective public policy as well as judicial and law enforcement framework these practices lead to effective strategies for protecting Critical Information Infrastructure.

The European Commission, ENISA, ITU and several of the Member States are leading initiatives with a promise to deliver a comprehensive cyber security framework. The key challenge will be in bringing all the key stakeholders onto a level playing field and collaborating across borders to develop a common approach.

Complex Adaptive Systems – an Approach to increase Dependability.

In this article we claim that complexity of critical information infrastructures can be exploited to improve their dependability when they are designed according to a complex adaptive systems method. Policy makers should select an adequate governance approach and stimulate infrastructure providers to adopt the CAS-Approach.

Semir Daskapan

Professor
Delft University of Technology, Delft, The Netherlands
e-mail: semird@tud.tudelft.nl,

Jolien Ubacht

Delft University of Technology, Delft, The Netherlands
e-mail: jolienu@tud.tudelft.nl

Introduction

We claim that complexity can be an opportunity for governance of critical information infrastructures instead of just a threat when a CAS approach is applied. In this CAS approach dependability solutions emerge from collaborating end user systems or nodes.

To apply this approach an information infrastructure should first be converted into a CAS. Governments could stimulate the adoption of a CAS-approach as an engineering concept or market parties can embrace the approach in order to gain contracts or to enhance their imago. We present as such five options for governance.

A critical infrastructure refers to the chain of systems that facilitate the flow of information, matter or energy. Its failure might cause high direct and/or indirect social, economic or ecological damage. Most of the physical infrastructures also rely on information infrastructures, like road traffic systems and integrated SCADA systems, which inspires us to consider the latter one as critical. Society depends on those critical information infrastructures (CII) and, subsequently, the vulnerabilities of these infrastructures have urged governments to launch initiatives to protect them. For example, the initiation of the European Dependability Development Support Initiative resulting in the European Warning Information System and the European Network and Security Agency. In addition, national governments have launched research programs to assess the vulnerabilities of their national information infrastructures. The Netherlands the KWINT report commissioned by the Dutch Ministry of Economic Affairs, showed that full protection is unattainable and that measures have to be taken to deal with this residual vulnerability.[1]

Common technical means to protect infrastructures focus on redundancy as well on non-redundancy techniques.[2] Those means range from prevention by monitoring and warning systems till backups and recovery mechanisms by each individual infrastructure provider. Those implementations are not flexible or durable.

Common means to protect infrastructures focus on redundancy as well on non-redundancy techniques. Those implementations are not flexible or durable.

Infrastructures undergo rapid changes due to market competition and changing end user demands.

[1] Luiijf, E., H. Burger, et al. (2003). Critical Infrastructure Protection in the Netherlands: A Quick-scan. EICAR Conference Best Paper Proceedings. U. E. Gattiker. Copenhagen:19.

[2] Avizienis, A., J.-C. Laprie, et al., "Fundamental Concepts of Dependability", Research Report N01145, LAAS-CNRS, 2001.

The current implementations of those means are, however, tailored and tied to a specific constellation or state of the infrastructure.

Once this constellation or state of an infrastructure is changed, i.e. new (hardware or software) components, new interconnections to other infrastructures or a new company strategy, another tailored implementation of those protection means is required.

In addition, many infrastructures are not isolated, but interwoven with other types of infrastructures. For example, telecommunication infrastructures use the electricity infrastructure and the information infrastructure, but also visa versa. As such changes in one infrastructure may have an effect on the other linked infrastructures. Even initially small flaws in one infrastructure could result in amplified problems in another, dependent infrastructures and bounce back. As a consequence of this 'butterfly effect', complexity increases, manageability decreases and vulnerability of such interwoven infrastructures increases. Those large conglomerates of infrastructures are sometimes so complex that their total reaction to certain local distortions becomes unpredictable.[3]

The number of distortions increases gradually with the number of infrastructures n in such a conglomerate, but the frequency of changes is at least n^2 due to their reciprocal effect. Due to this complexity it is hard, if not impossible, to react adequately to problems with traditional approaches.

Consequently, dependability of the infrastructure services suffers from the growing complexity.

Whereas complexity seems to oppose flexibility, in this paper we will show, and this is our claim, that this complexity can be the solution itself to improve dependability of the infrastructure services and that governments should stimulate the use of complex adaptive systems (CAS).

Recently more and more individuals are supporting this claim and are providing their specific self-healing solutions to infrastructures.[4,5]

According to some authors self-healing solutions shall be considered. We think such solutions will fail.

Despite their valuable specific proposals, we think that because of the bandwagon effect the adoption of such solutions will fail. Reaching out to the policy makers is however not the aim of many other authors, which is the ultimate goal of this paper.

CAS method stimulating Policy

We consider a complex adaptive system as a collection of interdependent rule - following agents with interactions resulting in system-wide patterns across the group.[6] The richness and volume of these interactions enables a complex system as a whole to undergo spontaneous self-organisation. Self-organisation is the emergence of a patterned outcome that no individual had planned, i.e. emergent behavior of the system. A characteristic is that no agent needs to be aware of the existence of the total space. In information infrastructures, each computer entity (CE) knows at most what kind of capabilities it has and how it can look for relevant information in the environment. Properties of CAS are: emergent behaviour, adaptation, specialisation, dynamic change, decentralisation and coopera-tion.[7] Our positive perception of complexity, in which complexity is exploited to solve problems, is supported by other groups such as the Santa Fe Institute.[8,9,10]

If we consider critical information infrastructures (CII) as complex adaptive systems, in which the computers function as agents that execute specific standard procedures, they are able to cooperate together such that self-organisation becomes more reachable. Any distortion in the infrastructure is then cleared, somehow, by the cooperating agents. Dependability solutions can then emerge bottom-up from the smaller constituents and not solely top-down from the conglomerate as a whole. Self organised dependability concepts for some computer systems and networks, also called self-healing information infrastructures, have been proposed by others.[11]

3 Amin, M., "National Infrastructures as Complex Interactive Networks," Automation, Control, and Complexity: New Developments and Directions, T. Samad and J.R. Weyrauch, eds., John Wiley&Sons, New York, 2000.

[4] Dashofy, Eric M., André van der Hoek, Richard N. Taylor, "Towards Architecture-based Self-Healing Systems", Critical Information Infrastructures Security, Italy, 2008.

[5] Gustavsson, Rune, Björn Ståhl , "Selfhealing and resilient critical infrastructures",Critical Information Infrastructures Security, Italy, 2008.

[6] Eoyang, Glenda, and Doris Jane Conway, " Conditions That Support Self-Organization in A Complex Adaptive System" , International Association of Facilitators, USA, 1999

[7] Wilensky, U., M. Resnick, "Thinking in Levels: A Dynamic Systems Perspective to Making Sense of the World," Journal of Science Education and technology, vol.8, no.1, pp. 3-18, 1999.

[8] Langton, C. G., C. Taylor, et al., Eds., Santa Fe Institute Studies in the Sciences of Complexity. Artificial life 2, Addison-Wesely, 1992.

[9] Dooley, K., T. Johnson, et al., "TQM , Chaos and Complexity," Human Systems Management, vol. 14, no. 4, pp. 1-16, 1995.

[10] Dooley, K., "A Complex Adaptive Systems Model of Organization Change," Nonlinear Dynamics, Psychology and Life Science, vol 1, no.1, pp. 69-97, 1997.

[11] George, S., D. Evans, et al., "Biological Programming Model for Self-Healing", ACM Workshop on Survivable and Self-Regenerative System, VA, 2003.

Self-healing public infrastructures, however, exist only as an idea, but actual implementations to support such propositions are still lacking. [12]

A possible explanation for this is the lack of an appropriate government policy to stimulate CII providers to use the CAS enabling standards, despite the fact that such an approach could be a fruitful alternative to the traditional policy approach. Instead of stimulating providers to improve the dependability of their (part of the) CII individually, we advocate the use of policy instruments to stimulate CAS engineering. In the traditional approach, policy instruments are used to regulate the output of the individual system, i.e. dependability, whereas in the option that we propose, policy instruments should be used to stimulate providers to adopt a specific method, i.e. CAS engineering, by which dependability emerges. This is a change in focus from output based (dependability) towards process based (method to reach dependability) governance. This change in focus is visualised in Fig. 1. The self-organised dependability that can be achieved in the second option is more efficient and effective.

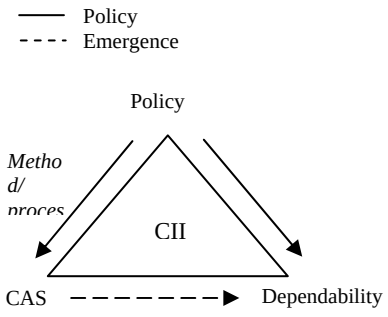


Fig. 1. Regulating dependability of CIIs

To reach this self-organised dependability a method is proposed.

The main purpose of this method is to convert a (part of the) CII into a CAS. In order to convert a CII into a CAS, the CII has to be defined as a system with cooperating computing entities or processors. This happens in four steps. First, the computing entities that are relevant to the problem at hand will be identified as agents. Second, a distinction will be made between the several roles of the agents, such that the system can be subdivided by a few clusters of similar agents. Agents of the same role have the same purpose in the CAS. Then, simple assumptions will be made about the behavior and knowledge of the agents within each cluster. Fourth, relatively simple similar tasks will be assigned to all agents within each cluster. Each cluster consists then of agents that are standardised, i.e. similar purpose, assumptions and tasks.

A CAS approach will only be able to function optimally if several actors cooperate in a communal adoption of standards to allow the system to work as a CAS.

The role of Governance - Policy instruments

A CAS approach towards complex information infrastructures is a way to enhance their reliability. However, a CAS approach will only be able to function optimally if several actors cooperate in a communal adoption of standards to allow the system to work as a CAS. But what if this stage of communal adoption is not reached, can governments play a role in stimulating its adoption, provided that governments recognise its potential? How can they stimulate its adoption by private market parties?

The first option is to rely on market forces, which means that the market in which private parties operate, will take care of the adoption and implementation of the CAS-approach.

This option is feasible in cases in which market parties feel a sense of urgency to collectively implement the approach and the market structure has the economic characteristics of effective competition. In the case of a dominant infrastructure provider that has many interdependent relationships in the sector, this dominant provider could function as a stepping stone for further adoption by dependent providers via conditions in its Service Level Agreements. When governments want to rely on market forces, then their activities will be limited to mediation or conversations with market parties to stimulate an industry protocol or code of practice; to the publication of performance indicators; to the operation of a complaint hotline or to conducting awareness campaigns for example for users of the infrastructure. These users in their turn can be stimulated to request for more resilience in the infrastructures. This requires well-informed users that are actually well organised enough to discuss this issue with the market parties who decide upon the adoption of a CAS approach.

The second option is (enforced) co-regulation, a situation in which infrastructure providers and government work together. Government will then draw the framework in which market parties can work towards adoption of the CAS approach. This option is an alternative to the situation that governments can impose formal regulation on the market parties and benefits of a communal adoption based on self-formulated terms are generally recognised.

The third option for governments is to use statutory or formal regulation based on relevant legislation. This option can function as a fall-back option in case all

[12] Amin, M., "Toward Self-Healing Energy Infrastructure Systems," IEEE Computer Applications in Power, vol.14, no.1, pp. 20-28, 2001.

Options for governance	Who and what is involved	When most appropriate?	Role for government	Reflection on success	Outcomes
Reliance on market forces	Individual customers and suppliers interact and achieve the best deal through the operation of market forces.	In markets with effective competition	Persuasion Mediation Conversation Performance Indicators Complaint Hotline Awareness campaigns	Market parties should feel a sense of urgency. Or a dominant, willing provider who can make demands via SLA with third parties. Or powerful users who can influence providers' willingness to consider CAS-approach	CAS-approach implemented via SLA Code of Practice/industry protocol
(Enforced) co-regulation	Regulator and stakeholders work together. The regulator determines the framework for stakeholders to work within. Enforcement powers exist but rarely used in practice.	When there are benefits to all parties or when benefits of a communal adoption based on self-formulated terms are generally recognised	Design of framework for reaching communal agreement for adoption	Benefits of communal adoption must be recognized by the market parties	Code of Practice/industry protocol
Statutory or formal regulation	Government applies statutory law to the case at hand or a regulator applies regulations based on relevant legislation and/or licences.	There are players with market power who control facilities; and there is a need for investigation into, and possible action against, anti-competitive practices	Legislation Regulatory intervention in case of market power	Market parties will be legally forced to adopt the CAS-approach. If communal benefits are not recognized or costs are considered too high: court cases to challenge the legal or regulatory intervention	Enforced solution by legal means, costs for adoption to be decided upon by government/ regulator
Self-regulation	Stakeholders (industry, consumer groups and others) take the initiative to co-operate for a general benefit. Regulator's role as observer (if any).	Sense of ownership of an issue among the market parties	Observer, initiating role	Co-operation among market parties based on communal recognition of the benefits of CAS-approach	Code of Practice/ industry protocol
Standardisation	Standardisation bodies such as IETF, IEEE and the organisations that take part (in specifically the security, reliability and trust committees)	When organisations taking part in the standardisation committee have a communal interest in the CAS-approach	Inform and communicate with standardisation bodies	CAS-approach becomes part of the agenda of security committees, uncertain outcomes as the (long) process of standardisation is influenced by strategic and political forces	International standard that includes or is based on CAS-approach. Adoption via implementation of the technical standard

Table 1 Options for governance, based on[15], adopted by the authors

other options fail. Or, in the case of a market in which one infrastructure provider has market power and

subsequently prevents the adoption, a regulator can enforce the adoption via a license condition or via formal regulation.

The fourth option is self-regulation, which entails that stakeholders take the initiative to co-operate on the adoption of standards for a common, shared goal. If a governmental body is involved (this is not necessarily so), it will be in the role of observer or first inspirator for the initiative. To conclude we will shortly reflect on the question how to choose between the five option(s)?

The choice of an arrangement in general depends on:

The fifth option is the route of standardisation. The role of government would then be to exert influence on the agendas of international standardisation bodies which are able to draw attention to the CAS-approach. The outcomes would be that the CAS-approach becomes part of a standard or at least becomes an issue on the agenda of the standardisation bodies such as the IETF, IEEE, and more specifically within the information security committees.

Depending on the market structure (few or many market parties), the sense of urgency and the willingness by market parties to implement a CAS-approach, the institutional setting and the required speed of implementation (in case of short term goals, a long term standardisation process is not suitable), governments can make a choice to stimulate adoption either with soft (e.g. persuasion) or harder (formal) tools for enforcement.[13,14]

On the other hand, private market parties such as ISP's can consider the opportunities to use a CAS-approach as a selling point (especially those ISP's who want to gain contracts with governmental bodies) or they can promote a Code of Practice or Industry Protocol that is supported by a majority of market parties responsible for security in critical information infrastructures as a construct that is beneficial for the industry's overall image. Exploration of the options should be creative and not limited to a one size fits all solution.

Choosing the right Policy Instruments

It should be noted that the appropriate type of governance could change over time.

If, for example, a national government decides to use formal regulation to stimulate the adoption of a CAS approach, this enforcing type of regulation can be changed into co-regulation or even self-regulation, when a specific level of adoption is reached.

1. the sense of urgency on the part of government and degree of dependency of society on the critical information infrastructure(s) in case. If both are high, then governments will be more inclined to apply statutory law or regulation (if at all possible in a liberalised market);

[13] Ayres, Ian, John Braithwaite. Responsive Regulation. Transcending theDeregulation Debate. Oxford: Oxford University Press, 1992.

[14] Ayres, Ian, John Braithwaite. "Designing Responsive Regulatory Institutions". *The* Responsive Community, vol. 2, issue 3, unnumbered pages,1992.

[15] Oftel. (2000b). Encouraging self- and co-regulation in telecoms to benefit consumers. London: Oftel, June 2000.

2. the action arena in which the decision to adopt a CAS approach has to be taken. Ostrom[16] identifies an action arena by
   a. the action situation: which and how many participants are involved, what information do they possess in order to take a decision, how will they assess the outcomes of the decision and what are the costs and benefits and
   b. the actors in that action situation: what are their preferences, which are their capabilities for information processing, what selection criteria will they apply and what are their resources?

   The arrangement has to fit with the character and structure of the action area.

   This requires a market review of the providers of (parts of) the critical information infrastructure at hand to start with.
3. the institutional framework in which government and private market parties operate. The most important questions are:
   a. is experience with co- and self-regulation or with industry already present? And do resources allow the fostering of these types of arrangements at all? In case of twice yes, then these options are more in the picture than when co- and self-regulation have to enter a world without prior experience with these arrangements;
   b. does government or the regulator have to discuss the adoption of the CAS approach with a limited number of market parties at the round table of negotiation or with an Industry Association? Or, on the contrary, is the market populated by a multitude of solitary private market parties that do not have a representative association? In the latter case, co-regulation can be problematic.
   c. What does the toolbox for statutory or formal regulation look like or in the case of co- and self-regulation: what does the toolbox for remedial action look like in case the arrangement fails?
4. the transaction costs of the arrangement (for enforcing and monitoring the arrangement) and
5. the investment costs to be made by private parties. If these are high, more resistance can be expected. However, if public resources are available to support the adoption of a CAS-approach, this resistance can be overcome.

Market structure, the sense of urgency, the willingness by market parties, the required speed of implementation and the institutional setting are criteria to select an appropriate governance option.

This list of considerations is merely indicative of the criteria that indicate that a comparative assessment of the governance options is not a straight forward one. In a liberalised market with market parties that compete but are not inclined to adopt a CAS approach to enhance the reliability of critical information infrastructures, it is tempting to conclude that governments have to legally enforce a CAS approach.

However, as we have shown, other options are available. Options that better fit with the liberalised market approach. Depending on the market structure (few or many market parties), the sense of urgency and the willingness by market parties to implement a CAS-approach, the institutional setting and the required speed of implementation (in case of short term goals, a long term standardisation process is not suitable), governments can make a choice to stimulate adoption either with soft (e.g. persuasion) or harder (formal) tools for enforce-ment.[17,18]

On the other hand, private market parties such as ISP's can consider the opportunities to use a CAS-approach as a selling point (especially those ISP's who want to gain contracts with governmental bodies) or they can promote a Code of Practice or Industry Protocol that is supported by a majority of market parties responsible for security in critical information infrastructures as a construct that is beneficial for the industry's overall image.

Exploration of the options should be creative and not limited to a one size fits all solution

Summary

Self-healing methods have been proposed earlier to deal with dependability of infrastructures. Despite of that governments do not play an active role in stimulating these methods and usually perceive complexity as a contradiction to dependability. In this article we claim that complexity of critical information infrastructures can, on the contrary, be exploited to improve their dependability when they are designed according to a complex adaptive systems method. As such, we advocate that that policy makers should stimulate infrastructure providers to adopt that method. This approach enables a bottom up self –healing dependability, which is a shift in policy orientation from merely focusing on the outcomes of a system (output governance) towards focusing on the technical operations of the system (process governance).

[16] Ostrom, Elinor; Roy Gardner and James Walker. "Rules, Games and Common- Pool Resources". University of Michigan Press, 1994.

[17] Ayres, Ian & John Braithwaite. (1992a). Responsive Regulation. Transcending the Deregulation Debate. Oxford: Oxford University Press.

[17] Ayres, Ian & John Braithwaite. (1992b). "Designing Responsive Regulatory Institutions". In: The Responsive Community, vol. 2, issue 3, summer 1992, unnumbered pages

Critical Financial Institutions, OSPs and Business Continuity Plans.

This is the first article in a series of three on how a best practice in software engineering, Test Driven Development (TDD), could become also a best practice for BCP writing at CFIs. This article shows how compliance with the ECIP Directive requires Operator Security Plans (OSP) include a BCP. Next articles will cover how to deal with high costs of some BC crisis scenarios, and how TDD could help.

César Pérez-Chirinos
Professor, Business Continuity Unit Manager, Banco de España

e-mail: cepeche@gmail.com

Abstract

This article is the first of a series of three. The series summarises author's experience of successful application of Test Driven Development (TDD) principles in the implementation of the Business Continuity Management (BCM) System in a Critical Financial Infrastructure (CFI): a central bank. This approach has been also useful in other central banks, both in Europe and Latin America.

The full series will include: (i) a Context section, explaining why CFI should have a strong BCM Programme if they want to assure compliance with future revisions of the ECIP Directive, (ii) a BC Plan (BCP) Maintenance Issues section, showing common problems arising to keep the BCP updated, (iii) a TDD of BCPs section, showing how to use TDD-like approach to solve issues in section (ii); and a Conclusions section

To mitigate the risk of lack of resilience due to inappropriate protection measures, the Council Directive 2008/114/EC assign strong responsibilities to the 'owners/operators of ECI.

Context

The European Programme for Critical Infrastructure Protection (EPCIP) aims to improve the ability of some basic European supplies (i.e. power, transport, etc) to be restored after serious disruptions caused by large scale impacts, before the damage caused by unavailability of supplies reach unacceptable levels.

These disruptions can be caused either by natural disasters (i.e. earthquakes, floods, etc), by accident (i.e. fire, operational mistakes, etc) or by deliberate attacks. In Business Continuity (BC) jargon, this ability to properly resume an interrupted production process is called *resilience*.

To mitigate the risk of lack of resilience due to inappropriate protection measures, the Council Directive 2008/114/EC of 8 December 2008 "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (The ECIP Directive) assign strong responsibilities to the 'owners/ operators of ECIs'[1] when the disruption of normal operation of such European Critical Infrastructure (ECI) could cause unacceptable damage to one or more different EU member state to the ECI location one.

One of such responsibilities is that "Operator security plans ('OSPs') or equivalent measures comprising an identification of important assets, a

[1] 'Owners/operators of ECIs' means, under the Directive, those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under the Directive.

risk assessment and the identification, selection and prioritisation of counter measures and procedures should be in place in all designated ECIs."[2]

Minimum OSP content must include "protection and prevention means […] implemented for [critical assets] protection" [3].

As "'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability"[4], the conclusion is that OSPs must include Business Continuity Plans.

Why not be more explicit on this fact?

Business Continuity Plan Maintenance Issues

Perhaps a good reason to be so shy about openly asking now ECIs 'owners /operators' (and CFIs in next years) for strong BCM practice is that cost of resilience is virtually unlimited. The second article in this series will discuss this hard issue in more detail. For now on, we will take for granted that an ECI must have a world class BCP, as objective proof of a strong BCM Program-me being in place.

What if an ECI don't have such a BCP? In real life, there will be many ECIs doing its best effort to achieve resilience, but without any systematic approach.

To make things harder, its critical nature would probably banned them from sharing best practices (and worse problems) with other ECIs.

In such problematic scenario, expecting compliance with, let's say, BS 25999 BCM standard would be unrealistic for EU member state authorities in charge of checking the BCP included within an ECI's OSP for Directive's compliance.

It seems so an obvious conclusion that one of the targets of the European Programme for Critical Infrastructure Protection should be the achievement of some degree of harmonisation in ECI's BCM, including required BCP content.

A Business Continuity Management Programme is a cornerstone for any Operator Security Plan as defined by the ECIP Directive.

Robustness of this cornerstone can only be achieved with a testing oriented BCM Programme

But this would not be a trivial task. BCP content suffers a chronic deficit of maintainability, so any effort to define it from a classical (i.e. legal) way will be probably doomed to failure. Meters of shelves plenty of thick binders would pass formal compliance at high production cost, without any real resilience improvement from present situation.

The current consensus within the BC experts' community is that robust and realistic BCPs can only be achieved as result of testing oriented BCM Programmes, complemented with intensive information sharing activities with peers, customers, suppliers and public authorities.

But even with PARSIFAL's like initiatives addressing information sharing within trusted groups, going from consultant's PowerPoint BCM presentations that convinced top managers to establish and support a permanent BCM Programme, to a full fledged BCP that can be fully tested *all the years*, in line with current recommendations, is a long process that can require three or more years in any complex organisation, as one can expect any ECI to be.

The Case of Critical Financial Institutions

Critical Financial Institutions, or CFIs, can be particular instances of ECI under the Directive, even if they are not formally designed as ECI candidates in current wording[5].

The "long and windy roads" of BCM are well known by CFIs, which are already working hard to align with the guiding principles behind the EPCIP Directive, without waiting for its revision in 2012[6]. There are some public proofs of this statement[7,8].

So, we can state that CFIs, like other ECIs sectors, are looking for effective and efficient strategies to maintain its BCP. This is the problematic that deserve the effort to take a look to Test Driven Development (TDD) as inspiration to design these solutions. This will be the focus of third and last article in this series. But, before explaining a solution, let's take a closer look to the problem.

First of all, a CFI wanting to have a first class BCM Programme need to have a very strong Disaster Recovery Plan (DRP) for its Information Technology

[2] CD 2008/114/EC, Whereas (11)
[3] CD 2008/114/EC, Appendix II
[4] CD 2008/114/EC, Article 2 (e)

[5] CFI were "first class" ECIs in early drafts of the ECIP Directive, where CFI was one of the eleven ECI Sectors listed in Annex I. Although the current Annex I only includes "Energy" and "Transport" ECI Sectors, it is expected that ICT return to Annex I by 2012, and perhaps also CFI.
[6] CD 2008/114/EC, Article 11.
[7] The ECB has been closely watching the ECIP Directive, to the point that it suggested some improvements to the security of the ECI catalogue (see **http://www.ecb.int/ecb/legal/pdf/c_11620070526en00010004.pdf**). Also very relevant to CFIs and BCM is this reference: **http://www.ecb.int/press/pr/date/2006/html/pr060609.en.html**
[8] In Spain, the BCM Consortium of the Financial Sector (CECON) is a leading actor in dissemination of BCM best practices. Some other EU member states' CFIs are in similar position.

and Communications (ICT) infrastructure.

In our case, we could characterise the ICT infrastructure a black box, able to commit two hours of Recovery Time Objective (RTO) and no data loss Recovery Point Objective (RPO) for all critical applications. This was a very strong foundation, built across twenty years of ICT investment; first formal DRP was available by 1997.

If you cannot build your BCM on something like this, you will need it first: no CFI today should be allowed to operate without a strong DRP. It can take a minimum of two or three years to reach the proper level. We guess that TDD could also help to build DRPs efficiently, but we can't prove it with a real case.

Next step, if you want to adhere to a BCM standard like BS 25999, you should perform a Business Impact Analysis (BIA) to identify the processes of your CFI and assign them a Maximum Tolerable Outage (MTO) and a RPO that the CFI stakeholders can accept. You should use MTOs to compute RTOs, subtracting the reaction time required to evaluate if the BCP need to be activated after a process interruption.

If you need to have an OSP ready in one year, as requested by the Directive, and you don't have a BCM Programme already in place, you don't have time to do a BIA: you should have done the BIA along the evaluation process[9] that concluded that your organisation was an ECI[10].

Unfortunately, it is quite possible that top managers underestimate the time required to implement the BCM Programme and perform the BIA. In such a case, you can do a "reverse engineering" of any contingency measure that is already in place to support your activities.

These contingency measures will give you a hint about what are the processes that are more relevant to the CFI stakeholders.

Conclusions (Part I)

We have shown in this article that Critical Financial Institutions should be already running mature BCM Programmes if they want to be ready for the foreseeable inclusion of CFIs in Annex II of the ECIP Directive in next revision planned by 2012.

We have identified also some problematic issues of running an effective and efficient BCM Programmes, which will be covered in next to articles in this series, including the use of Test Driven Development principles to address these issues.

IPR and Disclaimer

This article is a research item of the on-going PhD Thesis at Oviedo University of its author and does not express a position of Banco de España on the subject.

[9] CD 2008/114/EC, Article 3

[10] This is the equivalent problem to the 'Waterfall' classical software development process: most of the available time to build a system is spent trying to specify its requirements.

Are you in Control?

That was the key question discussed at the second Dutch Second Dutch Process Control Security Event at the Technical University of Delft, December 4, 2008.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl

The second Dutch Process Control Security Event attracted many process control people. The event was organised by the National Infrastructure against Cybercrime (NICC). Over hundred people responsible for the security of process control systems (PCS) and related networks in many of the Dutch critical infrastructures (CI) and key industries took part in the two plenary sessions and four parallel workshops. The event was co-located with the Production Process Automation (PPA) event for PCS/SCADA vendors and system integrators which was organised by the Dutch Federation for Technology Branches (FHI). They discussed a set of PCS issues including information security. At the end of the day, both events joined for a closing debate session on security and responsibilities.

Annemarie Zielstra, programme manager of the NICC opened the event. Besides the FIH, the WIB (Dutch PCS user association), and the Technical University of Delft participated in organising the event. In May 2008, the first process control security event identified a set of actions which set the agenda for this event: increase risk awareness by top management, sharing incident information, and establishing a common user - manufacturer view on PCS security requirements as part of the procurement process.

Currently it is unclear who is responsible for the information security of process control systems [Dutch CIO Platform]

She continued: "The PCS security issues in the Netherlands are not addressed in isolation. The Dutch PCS community is both involved in the European SCADA Security Information Exchange (Euro-SCSIE) and the newcomer MPCSIE (Meridian Process Control Security Information Exchange). The latter has recently been established by the international governmental ICT-policy discussion group Meridian."

"The question 'Are you in control?' needs to be answered by all Dutch CI and key industries. Some weeks before this security event, a meeting of the Chief Information Officers (CIO) Platform and the Director-General for Energy and Telecom of the Dutch Ministry for Economic Affairs took place discussing today's theme. That meeting showed that not all CIO know who in their organisation is responsible for the information security of control systems. When something goes wrong, the CIO will be probably looked at.

One CIO became aware of control systems in his organisation when he was planning a move of his computer room. Obviously, not all organisations are in control of the information security aspects of control systems!"

"As a result, the CIO Platform plans to take a coordinated action in The Netherlands to increase risk awareness amongst the Dutch CI and key industries. It should become crisp and clear who is responsible for process control security within each organisation."

The next agenda item was a plenary debate between Aad Dekker (Information security officer at NUON, a Dutch power distribution company) and Ted Angevaare, the SHELL global DACA (process control) security manager. Their views on process control security differed in details like their answers to the question "Is security the safeguarding against undesirable control of the process or is it the safeguarding against the disruption of the production?" Next was debated whether office ICT-security should include physical security and

whether the same approach holds for the process control environment as well. Screening of personnel, legal hacking as part of security audits, and formal reporting of incidents followed as topics. Regarding the latter, it was concluded that most organisations that use PCS do not have a rigid incident reporting scheme. Probably many incidents are not reported because the responsibility for the ICT-security side of PCS is not clearly organised in organisations. It is felt that motivating people about their work and security awareness is more important that taking sanctions against those who create a security breach. One of the debaters had to admit that he does not know how ICT-assets are decommissioned and whether computer media such as hard disks are properly wiped or destroyed.

Use your female intuition!

Is top management able to take the right decisions about ICT security? "Probably not", was the answer as incident reports are not complete, and responsibilities for process control security are not totally clear. The risk is that top management will overreact in case of an incident which hits the press. How to avoid that? "Steering and preparing them by executing proper risk assessments and risk management. Above all, avoid scaring talks to them by vendors who want to push sales." One also should avoid being to dependent of process control hardware and software vendors. Understand one's own needs and fix your vulnerabilities based upon your risk assessment. And put far less trust in third party PCS maintenance people than in your own people.

What is the role for government? The answers ranged from setting de facto security standards, assistance when fighting a cyber attack to a better information position by information exchange with and easy access to law enforcement, and intelligence services. Leading should be "what is in for both of us?"

Four workshops

The workshops were held in parallel and repeated after a break allowing participants to participate in two workshops of their choice. The four themes were set during the first PCS security event: good practices in the energy sector (by Randi Roisli, Norwegian StatoilHydro), social engineering (Jan de Boer, TIAS Business School), gaming and simulation (Mark de Bruijne, TUDelft), and the development of the Dutch PCS security incident database (Martin Visser, Waternet and Eric Luiijf, TNO and NICC).

Randi Roisli showed the highly complex, dependent PCS environment where a large set of operators and suppliers together control the oil production on a number of Norwegian off-shore and on-shore facilities. The joint Oil Industry Association (OLF) guideline 104 has been developed to address the process control security weaknesses, both organisationally and technically. A self-assessment tool assists the organisations in measuring their PCS security posture.

Jan de Boer is an ethical hacker who performs social engineering upon request. He showed the approach and the results of several cases. He pleads for using the "human (female) intuition" much more to avoid becoming tricked by a social engineering attack. Mark de Bruijne showed where different technologies meet each other in gaming-simulation. This new combined research field allows different actors, e.g., process control and ICT-departments, to learn from interactions between both departments in a simulated (risk free) environment. An example of a game to train dike patrol people was shown. Martin Visser presented the NICC context for sharing information about process control/SCADA incidents. Eric Luiijf continued by explaining the vision and long-term aims of a security incident database. Consultations with representatives of various NICC petals leads to a pragmatic approach: start as soon as possible, use a standard reporting form in English, anonymisation of incident reports by a trusted central body, and distribute the information to organisations which have agreed to keep the shared information secure. Details, especially the legal ones and the trusted party, still have to be worked out. Very worthwhile comments were received from the participants. Keep it simple, stupid and be pragmatic are considered the key to success.

Final debate

The final debate, organised by both NICC, WIB and FIH, brought together the PCS users, manufacturers, vendors, system integrators, and government. A main part of the debate circled around the responsibility for security. Users require more secure PCS, manufacturers and vendors have security knowledge, manufacturers point to PCS integrators as they do the configuration and integration of parts of multiple manufacturers, system integrators point to both the end users and the PCS manufacturers. "Security is dropped first when it comes to price while forgetting that cost reduction by using COTS software and hardware already has been cashed in". "Investments in security reduce downtime and increases production time." "Do not overlook the insider threat!" "Risk assessment shall be the driver, not regulations or laws. An independent regulator, however, may set the boundaries of a proper security posture for a critical sector." "Learn from the safety and security checklist for constructors (VCA) approach. Security can make organisations more efficient and effective!"

Obviously, this was not the last debate on this challenge, although some progress was made in understanding the background of the different positions. For that reason, the responsibility issue was selected as the main topic for the next NICC Process Control Security Event on April 23, 2009.

CRITIS'08 - Review of the 3rd International Workshop on Critical Information Infrastructures Security

The 3rd international workshop on CIs and their ICT from 13th to 15th of October 2008 in Rome continued the success of its predecessors and attracted researchers and professionals dealing with all kinds of large critical infrastructures

Program Co-Chairs:

Stefan Geretshuber

IABG mbH, Germany
InfoCom, Safety & Security,
Dept. for Critical Infrastructures
geretshuber@iabg.de

Roberto Setola

University Campus BioMedico, Italy
Complex System & Security Lab
r.setola@unicampus.it

The 3rd international workshop on Critical Information Infrastructures Security, CRITIS'08 was held from 13th to 15th of October 2008 at the marvellous "Villa Mondragone" in Frascati (Rome), Italy.

The workshop was focused on an interdisciplinary and multifaced dialogue about the third millennium security strategies for Critical Information Infrastructures (CII) and their protection. CRITIS'08 was aimed at exploring new challenges posed from CII, bringing together researchers and professionals from universities, private companies and public administrations interested in all security-related aspects and actively involved in the scientific communities at national, European and trans-European levels.

CRITIS'08 was co-organised by ENEA and the Italian Association of Critical Infrastructures Experts (AIIC). The program committee was composed by an international group of recognised experts in both information security and critical information infrastructure protection. The program committee received 57 papers that illustrated research results, R&D projects, surveying works and industrial experiences related to the subjects of the workshop. Compared to its predecessors CRITIS'08 received almost the same number of papers as CRITIS'07 but attracted with about 140 participants a larger audience than all its predecessors.

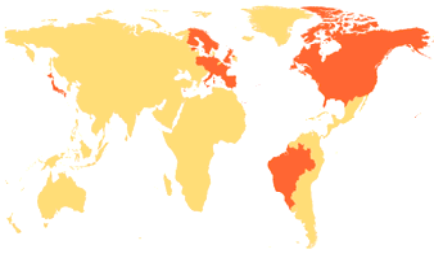
The audience of this year's workshop consisted of researchers and professionals from academia, industry and public administration from 21 nations.

CRITIS'08 attracted participants from 21 nations

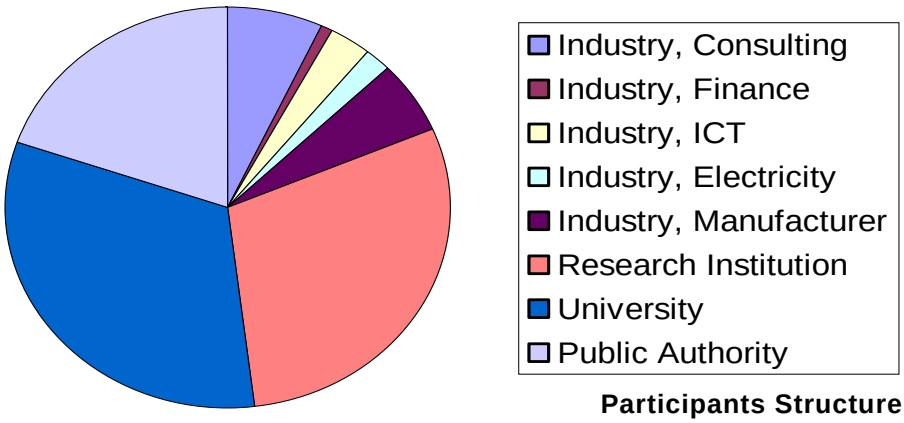
Within three days CRITIS'08 has presented 25 attractive high-quality papers arranged in six sessions, that have passed the thoroughly peer review process. Each session was chaired and introduced by invited talks given by very well known research personalities of the international Critical Infrastructure domain.

The venue - Villa Mondragone

The venue "Villa Mondragone" beauty-



fully situated next to Frascati round about 20 km southeast of Rome downtown has been the residence of Popes and famous families of the ancient nobility over the course of its long history. After a varied history the monumental complex has been acquired in 1981 by the University of Rome Tor Vergata. Nowadays the restructured section of the estate is the site for considerable national and international conferences and other important cultural events. With its wonderful gardens and magnificent view towards Rome Villa Mondragone has provided an excellent and exclusive surrounding for CRITIS'08.



Participants Structure

CRITIS'08 Day One

The CRITIS'08 workshop was opened with a warm welcome address by the President of ENEA, Prof. Luigi Paganetto. After his opening words Prof. Pagetto handed over to CRITIS'08 General Co-Chair Sandro Bologna - ENEA (Italy) who moderated all three days of the workshop.

The scientific program of CRITIS'08 started with the invited talk about "Modelling and Simulation of Critical Infrastructure" by Prof. Erol Gelenbe – Imperial College (UK).

The following Session 1 "Modelling and Simulation" also was chaired by Prof. Gelenbe.

The first paper introduced the work of Francesca Mariani et al. about a mathematical model for blackouts of high voltage electric networks. In the second paper Vincenzo Fioriti, ENEA (Italy) presented a method how to depict the stability of a distributed generation network using the Kuramoto models. The "Modelling and Simulation" session was closed by a paper, presented by William Tolone, of the University of North Carolina at Charlotte (USA) about system of systems analysis for critical infrastructure behaviours.

Session 2 "Dependency analysis and modelling" was chaired by Adrian Gheorghe (Old Dominion University, USA). Rüdiger Klein from Fraunhofer IAIS (Germany) opened this session with his presentation about information modelling and simulation of large interdependent critical infrastructures. Afterwards the work of Mario Beccuti et al described the multi-level dependability modelling of interdependencies between the electricity and information infrastructures.

Next the work related with interdependency analysis in electric power systems done within the EU project CRUTIAL was presented by Felicita Di Giandomenico, Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo" (Italy).

In the final paper of session 2, presented by Emiliano Casalicchio, University of Roma – Tor Vergata (Italy) described a federated agent-based approach for modelling and simulation of complex interdependent systems.

The first day was closed by a welcome cocktail and a modern free jazz concert which was exclusively composed for the CRITIS'08 workshop. The subject of this unique concert was directly related to the subject of the workshop. The music was composed to create a suitable atmosphere and the words were inspired by many events reported in the newspapers in 2008 and also by classical literature.

CRITIS'08 Day Two

On Tuesday 14th of October the workshop continued with invited talk about "Resilience and Self-healing challenges" by Prof. Massoud Amin – University of Minnesota (USA).

Within the following third session "Increasing resilience and self-healing" chaired by Massoud Amin different approaches how to implement resilience and self healing capabilities were presented.

Rune Gustavsson, Blekinge Institute of Technology (Sweden) informed about the


Villa Mondragone

understanding of self healing and resilient critical infrastructures within the FP6 project INTEGRAL. Yves Deswarte, LAAS – CNRS (France) presented the work of the EU CRUTIAL project regarding critical infrastructures security modelling, enforcement and runtime checking. Salvatore D'Antonio, Consorzio Interuniversitario Nazionale per l'Informatica (Italy) introduced in his paper the INSPIRE project about increasing security and protection through infrastructure resilience. In the last paper of this session, Stefan Geretshuber, IABG (Germany) presented a method to increase of power system survivability through a decision support tool "CRIPS" that is based on network planning, developed within the FP6 project IRRIIS.

The following special session, chaired by Rüdiger Klein – Fraunhofer IAIS (Germany) presented the IRRIIS project. IRRIIS is a European integrated research project started in February 2006 within the 6th Framework Programme. It will be finished in July 2009. The aim of IRRIIS is to develop methodologies, models and tools for the analysis, simulation and improved management of interdependent Critical Infrastructures (CIs). Middleware Improved Technology (MIT) will provide new communication and information processing facilities in order to manage CI dependencies. At the end of three years project life time IRRIIS will have contributed to increase dependability, survivability and resilience of EU ICT-based critical information infrastructures.

The third invited talk, "Risk and Decision Analysis in Infrastructure Protection" by Prof. George Apostolakis MIT (USA) introduced the forth session about "Vulnerability and risk analysis" also chaired by George Apostolakis.

This session emphasised methods and tools for risk assessment in complex networks like power grids or railway networks.

In the first paper of this session by Ettore Bompart et al informed about the assessment of structural vulnerability for power grids by network performance based on complex networks.

The next presentation introduced the work of Francesco Cadini et al about a method to rank the importance of the components of a complex network infrastructure by using centrality measures. The following paper, by Selan Rodriques dos Santos and Joao Paulo S. Medeiros presented RadialNet, an interactive network topology visualization tool with visual auditing support. Session 4 was closed by a paper about quantitative security risk assessment and management for railway transportation infrastructures introduced by Francesco Flammini et al.

After session 4 additional 16 papers have been presented in a well attended poster session. There was time to answer open questions and for fruitful discussions and it was a platform for exchange.

The second day of the CRITIS'08 was concluded by the exclusive gala diner at roof garden of the Hotel Exedra located directly at Piazza della Republica in Rome downtown. The day ended after the gala dinner with the "Rome at Night Tour", a guided bus tour trough the city. The participants were brought to the following sites: Colosseo, Circo Massimo, Bocca della Verità, Isola Tiberina, Castel Sant'Angelo, Basilica di San Pietro, Gianicolo.

CRITIS'08 Day Three

On Wednesday CRITIS'08 workshop continued with the fourth invited talk about "Cyber threats and vulnerabilities", by Andrea Vilboni Microsoft (Italy). Within the following session 5, "cyber threats & SCADA" chaired by Stefano Panzieri (Università di Roma Tre, Italy) information about SCADA related security issues, protocol security analysis and power control system test beds were presented.

Eric Luiijf, TNO Defence, Security and Safety (Netherlands) informed about measures and methods to assess and improve SCADA security in the Dutch drinking water sector.

Tiago H. Kobayashi, DCA/UFRN (Brazil) presented a study about the influence of common IT malicious traffic on Modbus/TCP communications. Igor Nai Fovino, Joint Research Centre (Italy) informed about the research efforts done by JRC regarding SCADA malware. Giovanna Dondossola, CESI RICERCA (Italy) introduced in the last paper of

Round Table

session 5 efforts regarding existing test beds for assessing critical scenarios in power control systems done within FP6 project CRUTIAL.

The sixth and final session "security and crisis management" chaired by Sujeet Shenoi (University of Tulsa, USA) focused on approaches for incident response management, policy – making for infrastructure protection and strategy analysis for critical information infrastructures.

Martin Gilje Jaatun, SINTEF ICT (Norway) introduced in the first paper of this session a structured approach to incident response management in the oil and gas industry.

In the next paper, the work of Semir Daskapan et al about a method for information infrastructure protection by technology driven policy were presented. The following talk from Jose Torres et al informed about security strategy analysis for critical information infrastructures. In the last paper of session 6, the work of Mikael Asplund et. al. about Information Infrastructures - Cooperation in Disasters was presented.

Invited talk 5 "Strategies for Securing Interconnected Critical Infrastructure Networks" by Prof. Sujeet Shenoi University of Tulsa (USA) and invited talk 6 "European strategy for Critical Infrastructure Protection research", by Angelo Marino, DG Information Society and Media (European Commission) completed the CRITIS'08 workshop program.

As the final highlight of CRITIS08, the round table opened the stage to discuss on the current and future challenges of Critical (Information) Infrastructure Protection. The round table was moderated by Roberto Vacca (middle) and attended by recognised international experts from industry, research and politics (left to right):

- Angelo Marino – DG Information Society and Media (European Commission),
- Adrian Gheorghe – Old Dominion University (USA),
- Paul Friessem – Fraunhofer SIT (Germany),
- Luisa Franchina – Italian Civil Protection Department (Italy),
- Rainer Krebs – Siemens (Germany),
- Genseric Cantournet, – Telecom Italia (Italy),
- Eric Luiijf –TNO (The Netherland),
- Marc-Alexandre Graf - Swiss Federal Office for Civil Protection Switzerland).

Summary

CRITIS'08 General Co-Chair Sandro Bologna - ENEA (Italy) summarized in his closing words that the workshop again has been successful in different ways. On the one hand the workshop hosted high-quality peer-reviewed papers and remarkable invited talks which attracted the interests of all the attendees. On the other hand the CRITIS'08 like their predecessors successfully brought together both academia and industrial experts to share their different points of view how to face the current and future challenges of critical (information) infrastructure protection.

Besides the high-quality scientific contend of CRITIS'08 workshop, the marvellous workshop location of "Villa Mondragone" and the elegant Gala Dinner in Rome contributed to make the outstanding event memorable for a long time.

Additional information

The complete program of the workshop along with all the slides together with some pictures and movies collected during the workshop can be found at http://critis08.dia.uniroma3.it.
Additionally post-proceedings will be published by Springer in the Lecture Notes in Computer Science series until summer 2009.

Outlook CRITIS'09

After the success of CRITIS'08 the steering committee has announced the granted mid-term continuity of the CRITIS workshop series. The next CRITIS workshops will take place end of September 2009 in Bonn, Germany and 2010 probably in Lucerne, Switzerland.

CRITIS'09 will be organised by Fraunhofer IAIS which is one of Germany's leading institutions for research and development of innovative information systems. One of the institute's main areas is preventive security with a whole bunch of EU, governmental and industry funded projects in this domain. Fraunhofer IAIS is the project coordinator of the EU Integrated Project IRRIIS and the FP7 project DIESIS.

The location of CRITIS'09 Bonn is the former German capital and still hosts half of the German federal ministries, plus many security related offices, including the German Federal Network Agency and the German Federal Office for Information Security (BSI) as well as the Federal Office of Civil Protection and Disaster Assistance (BBK). Bonn is also the headquarters of German Telekom, T-Mobile, and the German Post. All in all, Bonn is an ideal location for a workshop like CRITIS. The venue of CRITIS'09 will be the Günnewig Bristol Hotel, located in Bonn's city centre.

For further details please visit http://www.critis09.org.

ECN-12 Selected Links and Events

Upcoming CIIP Conferences in Europe

- Information Day on Objective 1.4 Trustworthy ICT, 18 June 2009, Brussels, Belgium http://cordis.europa.eu/fp7/ict/security/events_en.html
- 6th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, July 9 / 10, 2009, Milan Italy http://security.dico.unimi.it/dimva2009/index.html
- 5th International Conference on IT Security Incident Management & IT Forensics, September 15th to 17th, 2009 Stuttgart, Germany http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2009
- 4th International Workshop on Critical Information Infrastructures Security Bonn St. Augustin, Sept. 29-Oct 2,2009 http://www.critis09.org

Selected Links from Articles of this issue

- General policy linked to EPCIP and a directive focusing on the identification and designation of pan-European Critical Infrastructures : http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm)
- European Security Research Conference is expected to deliver its final recommendations in autumn of 2009: http://www.esrif.eu/index.html
- New promising research directions for the constituency to be addressed in the next few years: http://cordis.europa.eu/ist/trust-security/projects.htm.
- Joint effort between the FP7 ICT and Security Programmes: http://cordis.europa.eu/fp7/ict/ and http://ec.europa.eu/enterprise/security/index_en.htm
- Technical details on actual research projects: http://cordis.europa.eu/fp7/ict/critinfpro/projects_en.html.
- **DIESIS** project aims at establishing the basis for a European modelling and simulation e-Infrastructure to foster and support research on all aspects of CIs: http://www.diesis-project.eu
- Microsoft security advice: http://www.microsoft.com/security/default.mspx
- The Trustworthy Computing Security Development Lifecycle: http://msdn.microsoft.com/en-us/library/ms995349.aspx
- Microsoft's Security Intelligence Report version: http://www.microsoft.com/presspass/newsroom/security/factsheets/04-08SIRv6FS.mspx
- End-to-End Trust vision SAFECode: http://www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx
- Software Assurance Forum for Excellence in Code http://www.safecode.org
- Industry Consortium for the Advancement of Security on the Internet ICASI: http://www.icasi.org
- The ECB has been closely watching the ECIP Directive, to the point that it suggested some improvements to the security of the ECI catalogue: http://www.ecb.int/ecb/legal/pdf/c_11620070526en00010004.pdf
- Further References on CFIs and BCM: http://www.ecb.int/press/pr/date/2006/html/pr060609.en.html

E-Reports and EU funded Research Projects

- The Royal Academy of Engineering published its report Dilemmas of Privacy and Surveillance in March 2007: www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf
- The interdependencies of payment and settlement systems: http://www.bis.org/publ/cpss84.htm
- CRITIS 08 complete program of the workshop along with all the slides together with some pictures and movies collected during the conference can be found at http://critis08.dia.uniroma3.it/
- FP7 PARSIFAL Coordination Action project brings together CFI and Trust and Security research stakeholders contributing to the understanding of CFI research and development challenges: http://www.parsifal-project.eu
- FP7 CoMiFiN Strep projects goal is to create a federated, distributed and collaborative network of agents for enhancing trustworthiness and dependability of financial infrastructures: http://www.comifin.eu