1/2011

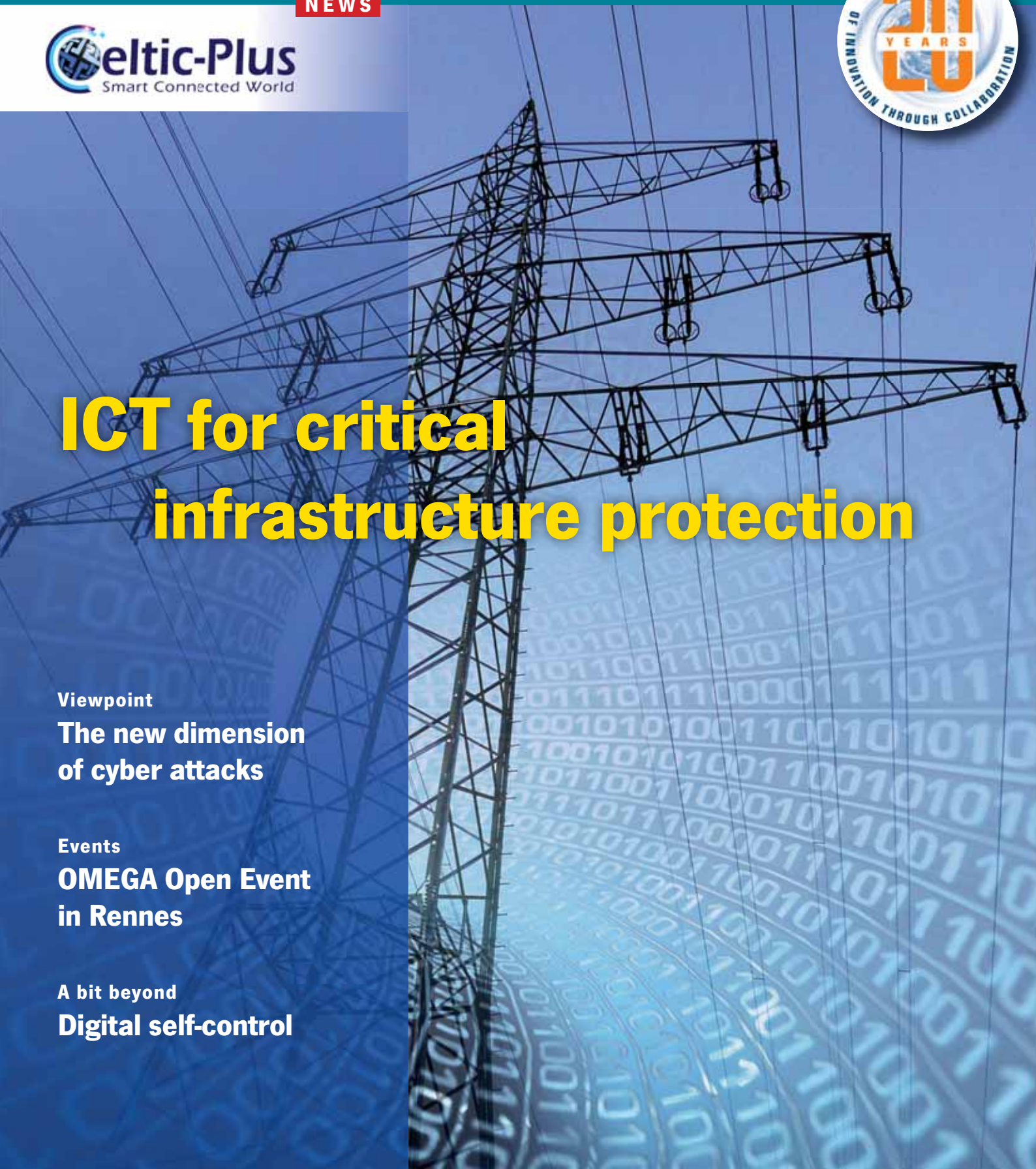
EURESCOM mess@ge

The magazine for telecom insiders

NEWS

Celtic-Plus
Smart Connected World

20 YEARS OF INNOVATION THROUGH COLLABORATION



ICT for critical infrastructure protection

Viewpoint
The new dimension of cyber attacks

Events
OMEGA Open Event in Rennes

A bit beyond
Digital self-control

EURESCOM

Eurescom Management Support for FP7 Projects

You focus on research – We take care of the adminstrative burden

Should researchers spend a lot of time on the administrative details of the Seventh Framework Programme? We don't think so. We think researchers should focus on research and leave administrative details to specialists.

Eurescom has long-term experience in providing professional support for coordinators of European research projects. Our professional support tools for coordinators of European research projects have been continuously developed and further improved for more than ten years..

Scope of support services

Our support services include:

Controlling and reporting

- Controlling of planned/spent efforts and resources
- Tracking and chasing inputs for periodic work reports
- Preparing reported data for reports to the Commission
- Tracking and collecting financial statements
- Tracking, chasing and collecting due deliverables
- Reviewing and improving formal quality of deliverables

Communication and events

- Editing and maintaining of the project's Web content
- Maintaining mailing-lists
- Planning and supporting audio-conferences and web-conferences
- Coaching of audio-/web-conference moderators to make remote meetings more effective
- Organising the logistics of project workshops and other events

How to get our services fully funded

Our management support services for your FP7 project are eligible for 100 percent funding. Just reserve a small amount of the budget in your project proposal for our sub-contractual services, and once your project is accepted, our services get fully funded by the European Commission.

Contact and further information

Please contact us via e-mail at services@eurescom.eu to discuss the management support services you need and get a cost estimate or offer for your project.
Further information is available on our Website at
http://eurescom.eu/services

Celtic-Plus
Smart Connected World

Celtic-Plus

The complementary programme for Future Internet projects

Call deadlines in May and October 2011

Good news for proposers of Future Internet projects: Celtic-Plus, the successor of EUREKA Cluster Celtic, started in January 2011 and has launched two calls for proposals. The first call has a submission deadline of 9 May 2011, and the second call deadline is 10 October 2011.

Future Internet use case factory

The two calls in 2011 aim particularly at establishing the "Celtic-Plus Future Internet use case factory". The "factory" is complementary to the first Future Internet PPP Call under the EU's Seventh Framework Programme (FP7). There are many more excellent Future Internet use case projects to be expected than can be funded under FP7, and Celtic-Plus offers another opportunity to realise some of these.

Fast call process

For both calls full proposals are required showing the ambition of the proposal from the objectives through the time plan and partners to the expected results.

The projects will be evaluated, and those reaching the required standards will be retained and given the CELTIC label. The.start of the selected projects is scheduled to be within 4 to 6 months after the Celtic-Plus labeling. Please check the Celtic-Plus website for call details and the Celtic-Plus Purple Book.

Further information

For further information, please contact Heinz Brüggemann, director of the Celtic Office, at brueggemann@celticplus.eu
http://www.celticplus.eu

Dear readers,

In many respects, 2011 is a special year – on global and European level, for the ICT sector, but also for Eurescom.

On a global level, we have witnessed the revolutions in Tunisia and Egypt, in which courageous citizens have successfully claimed power for the people, forcing long-term autocrats to give way for a political change. Information and communication technologies have played an ambiguous role in these revolutions, as particularly the Internet was used both by the protesters to organise themselves and get access to information, but also by the autocratic regimes to spy on citizens and – by switiching off Internet access – blocking citizens from information.

On European level, the ongoing efforts to revive the European economy and deal with the effects of the economic crisis in some countries as well as the efforts to restore the stability of the euro could become crucial for the future of the European Union. As part of the EU's Innovation Union plans, the Future Internet could become a central element for strengthening Europe's competitiveness and reclaiming a place at the forefront of technological progress.

In spring 2011, the projects of the Future Internet public-private partnership programme will start within the EC's Seventh Framework Programme (FP7), and hopes are high that this programme will help European industry to strengthen its role in the important area of the Internet of the future. Europe faces strong competition from America and Asia on technologicial leadership in the future Internet domain and ICT in general. Thus, being at the technological forefront will have a direct impact on competitiveness.

In this context, there is a small company based in Heidelberg, Germany, which has been instrumental in orchestrating the Future Internet discussions from the end of industry: Eurescom. The year 2011 has special importance for Eurescom, as the company celebrates its 20th anniversary. On 14 March 1991, Eurescom was founded by 26 major European telecoms network operators.

Since then, a lot has changed – the telecoms market, information and communication technologies and the way people use them as well as Eurescom's business model. What has not changed in all these years, is the need of major European players in the ICT domain to collaborate on areas of common interest and Eurescom's dedication to enabling and supporting innovation through collaboration in ICT.

Today, this need to collaborate in research and development is more important than ever. Europe and the world are facing complex challenges, and ICT is part of the solution in addressing them. Whether it is energy efficiency for a more sustainable way of working and living or improving ailing healthcare system through e-health applications or solving transport problems through new mobility solutions – the contribution of ICT is and will be important for addressing major economic and social challenges in developed and developing countries.

One of these major challenges is the protection of critical infrastructures. In this issue's cover theme, we highlight some of the latest solutions, European research has to offer in making our critical infrastructures more secure. The relevance of the cover theme has been dramatically highlighted by the recent earthquake and the ensuing nuclear disaster in Japan.

This issue also includes articles on a number of other topics, and I hope you enjoy reading them. My editorial colleagues and myself would appreciate your comments on this issue and suggestions for future issues.

Milon Gupta
Editor-in-chief

Events calendar

29 – 30 March 2011
Celtic-Plus Event 2011
Heidelberg, Germany
www.celticplus.eu/Events/Event2011

17 – 19 April 2011
Tridentcom
Shanghai, China
www.tridentcom.org

16 – 19 May 2011
Future Internet Week
Budapest, Hungary
www.fi-budapest.eu

15 – 17-June 2011
Future Network & Mobile Summit 2011
Warsaw, Poland
www.futurenetworksummit.eu/2011

2 – 7 September 2011
IFA 2011
Berlin, Germany
www.ifa-berlin.com

9 – 13- September 2011
IBC 2011
Amsterdam, The Netherlands
www.ibc.org

12 – 16 September 2011
Future Internet Symposium (FIS)
Berlin, Germany
www.fis2011.org

27 – 29 September 2011
NEM Summit 2011
Torino, Italy
http://nem-summit.eu

4 – 7 October 2011
ICIN
Berlin, Germany
www.icin.biz

5 October 2011
Net!Works General Assembly
Brussels, Belgium
www.networks-etp.eu

Sn@pshot

Run, robot, run!

A knee-high robot called Robovie-PC has narrowly won the world's first full-length marathon for two-legged robots in February 2011. Robovie-PC crossed the finish line in the Japanese city of Osaka just a second before its closest rival after more than two days of racing. The 42 km race involved 423 laps of an indoor track at an average speed of 0.77 km/h.

Contents

NEWS

Celtic-Plus

Imprint

EURESCOM mess@ge, issue 1/2011 (March 2011)
ISSN 1618-5196 (print edition)
ISSN 1618-520X (Internet edition)

Editors: Milon Gupta (editor-in-chief), Peter Stollenmayer, Anastasius Gavras, Uwe Herzog

Submissions are welcome, including proposals for articles and complete articles, but we reserve the right to edit.
If you would like to contribute, or send any comments, please contact:
Eurescom mess@ge · Wieblinger Weg 19/4 · 69123 Heidelberg, Germany
Phone: + 49 6221 989-0 · Fax: + 49 6221 989-209 · E-mail: message@eurescom.de

Advertising: Luitgard Hauer, phone: +49 6221 989-405, e-mail: hauer@eurescom.eu
Eurescom mess@ge is published three times a year. Eurescom mess@ge on the Web: www.eurescom.eu/message

Malware – Can we stop this crime?

David Kennedy
Director of Eurescom
kennedy@eurescom.eu

I have recently experienced a malware attack on our home PC. I know I am not alone in this, as recent EU statistics show that more than 30 percent of us have had similar experiences. However, this was personal – they were in our family computer! One of my teenage daughters was confused by a trick question in a Windows-like box and, by clicking "No" to an obtuse question, she managed to initiate an attack from "Spyware Protector".

Now this scam is nasty. It is so clever that it bypasses your virus checker and actively prevents you from running system tools. It disables a surprising number of support functions, generates false virus reports, and does even not allow you to delete it. Then it pretends to be a real spyware/virus removal programme and uses very persuasive professional looking screens to ask you to pay money if you want to remove the viruses.

I was angry at this programme taking control of my PC and demanding money to give it back. The same thing happened to my parents' PC in Ireland, and they simply stopped using their computer as they did not know what to do. This is clearly wrong.

If I was to stop you in the street and tell you that you can't proceed unless you pay me money, you would be the first to call the police and have me arrested for blackmail, intimidation, assault with menace and demanding money. And the police would probably agree and lock me up.

However, if I occupy your computing resources and demand money to release them, you immediately tend to think in terms of virus checkers, malware removal and other remedial actions as if the user is at fault. But are we missing something? What else can we do?

We can look at the real world for advice: Germany has a rule on letter boxes that makes it clear when the owner has a sign saying "No advertisements", you are not allowed to put ads in there. Germany introduced a similar law with high penalties for phone calls from cold callers pushing unwanted contracts on people. There are rules for the Internet, but it is not clear if they are enforceable, and they vary from country to country.

What we should do

The first thing is to try and step out of our current PC/Internet conditioning. Right now if your computer and Internet connection do not work, you set about repairing it on the basis there is a fault in the complex set of programmes and functions in your machine. However, in the case of malware, there is no fault. A third party is taking control of your assets.

Normally we describe this as stealing and call the police. So why do we not think of calling the police about malware? I managed, with some difficulty, to find the web site where the German police invite us to report such malicious behaviour. Even then I hesitated as I did not know what the consequences of this would be. What if they want my computer for evidence? Will the law then deprive me of the use of my computer in the interest of securing evidence, just as the malware did trying to exhort money?

So to overcome these problems, we have to take two types of action:

1. The first is to recognise the crimes.
   Who has ever reported a virus or malware attack to the police and what will the police do? Should we report every such attack? Yes! And the more people report incidents, the sooner such things can be policed. The laws need to be tested in court.
2. The second is to have laws that can act without making things worse for the victims.

Evidence should be simple to obtain – certified scan results should be sufficient for prosecution. The "Software Protector" type guys should be liable to high fines for each attempted forced sale under European law. Europe should have rules for following such criminals outside of Europe too, so they cannot hide.

Come on Europe, protect the citizens with simple rules that encourage reporting of these crimes! An alternative is that we stop using the open Internet and divide it into safe walled gardens where we only communicate with those we know and trust, but this will kill Internet freedom quicker than any net neutrality debate.

Conclusion

We need to increase our recognition of, and reaction to, cyber crime – it is not only criminal when they steal your money or your identity; it is also criminal when they use malware to damage your property and steal your time.

P.S. I did manage to get "Spyware Protector" out of my computer without paying the ransom – but I haven't reported it to the police yet!

20 years of innovation through collaboration

The 20th anniversary of Eurescom

Milon Gupta
Eurescom
gupta@eurescom.eu

For humans today, 20 years is a very young age. In the fast-changing ICT sector, however, 20 years is a long time in which fundamental technological changes with deep socio-economic impact can happen.

The past 20 years have been the most dramatic in the field of personal communications, particularly due to the rise of the Internet. Never before in the history of the planet has so much information been available to so many people. This communications era is being pushed by young Internet companies like Google (age: 12) and Facebook (age: 7).

However, some parts of the revolution we see today have come from the traditional communications providers, and Eurescom had its share in facilitating this. As Eurescom celebrates its 20th anniversary in 2011, the company can look back on two decades of stimulating and facilitating technological progress in the European telecoms sector.

The beginnings of Eurescom

On 14 March 1991, Eurescom was founded by 20 major European telecoms network operators in Heidelberg, Germany. In the new context of liberalised telecoms markets, leading European telcos saw the need to explore technological challenges and opportunities of common interest via a joint organisation. Eurescom became the initiator, knowledge exchange platform and project management organisation for hundreds of projects that helped telecoms operators keep pace with the technological development.

Hot topics in the early days were interoperable European ISDN, ATM broadband solutions, new service areas, standards for DECT, and the design of network management systems. Later, the development of new services and applications for mobile and fixed networks as well as specifications in the Internet domain were added to Eurescom's fast-growing project portfolio.

Expanded scope after 2001

The bursting of the Internet bubble in 2001 changed the landscape for Eurescom. Its economically hard-hit member companies in the telecoms sector cut their research budgets for collaborative R&D. In turn, they encouraged Eurescom to diversify its activities into professional project and programme management in the open market. Since 2002, Eurescom has been an active player in the European Union's Framework Programmes, and in 2003, Eurescom was part of a core group initiating the first EUREKA Cluster on telecommunications called Celtic, this year succeeded by Celtic-Plus.

With the expertise of its multi-cultural and multi-disciplinary staff, Eurescom also has supported other R&D initiatives through its comprehensive management services and tools, for example the Wireless World Research Forum (WWRF), the Digital Media Project (DMP), and the recently founded Eureka Cluster for water management, ACQUEAU.

David Kennedy, director of Eurescom (right), discussing the future of the Internet with José Manuel Barroso, President of the European Commission.

Since the early work of drafting the Bled Declaration on a European approach to the Future Internet in 2008, Eurescom has been a driver of the Future Internet initiative leading to the formation of the Future Internet Public Private Partnership. This FI-PPP is now being implemented as a dedicated sub-programme under the EC's Seventh Framework Programme (FP7).

Outlook

Although comparatively old at age 20 in Internet-industry terms, Eurescom has managed to adapt its business model and service offerings to the fast-changing challenges and opportunities. The company maintains core principles of delivering high value collaboration for innovation and understands well the importance of effective management for the success of innovative projects. Both skills – clever collaboration and management excellence – will be needed more than ever, in order to help private and public European ICT players explore and exploit the technological opportunities for the next 20 years and, thus, Eurescom plans a lot of interesting projects and initiatives to help its customers stay globally competitive.

Eurescom study programme

More studies on future topics

Anastasius Gavras
Eurescom
gavras@eurescom.eu

The Eurescom study programme is a unique way of performing collaborative research between telecom operators. The programme was established almost 20 years ago and continues to be attractive for its members for addressing emerging topics in a short time frame. The latest study started in December 2010, and the call for new studies is now open.

Quick study results

The Eurescom study programme continues to be popular among the engineers and scientists of its member organisations. Especially in view of the diverse initiatives and activities on the Future Internet, the members of the programme can benefit from the studies. They can help them to quickly and flexibly define work items on topics that emerge and which need to be discussed and elaborated with engineers and scientists in other telecoms companies to develop a common opinion, position or statement. The programme is financed by its subscribing member companies, and their commitment is underwritten by their upfront payments to the programme's budget.

Competitive advantage

The fundamental working principle within the Eurescom study programme is collaboration. Any network operator or service provider may become a subscriber of the study programme and participate in it, if they share the interest of addressing the substantial issues facing the telecoms industry in a collaborative way. The results of the studies are exclusively available to the members of the programme so that the study subscriber organisations get a direct competitive advantage from collaborative work. The programme is flexible to accept study proposals at any time.

Study on Android security issues

In December 2010, Eurescom launched a study on security issues of the Android operating system, with a focus on the operator's view.

The nature of Google's Android operating system, which is broadly available on mobile devices, allows the users and application developers to assume full control over the devices, but also attacks on the operator's network. Although currently all impacts on the operator's network are caused rather by poorly written applications and fast dormancy issues, the framework makes it easy for malicious entities to attack the network and cause trouble.

The operators' core business is managed, secure communication, and most operators are developing value-added services and enablers on top of this core functionality. In this respect Google's role as information hub interferes with this role. An additional concern is that Google's understanding of customers' privacy is different from the telecom operators' understanding.

The study aims at developing a set of recommendations and a strategy on how to address and possibly solve the security and privacy concerns and, thus, safeguard operators' interests.

The study is intended to scope out the threats that certain characteristics of the Android operating system represent for network operators and potentially seed an initiative among operators to create a joint position regarding best practices in this area.

Recent studies

Other recent studies that will conclude in 2011 address a wide range of topics, like "Opportunities and challenges for operators in the mobile cloud", "Dynamic service discovery and use in a cloud environment", "Virtual customer premises equipment (CPE)", "Unified standardisation framework for telecommunications network enablers" and "Energy efficiency - Business opportunities for telecom operators".

Outlook

Currently, the first call for studies in 2011 is open, and proposals can be sent to Eurescom following the established procedure. Interested telecoms network operators can join the study programme anytime, and they can directly participate.

More information about the ongoing programme as well as past studies can be found at http://www.eurescom.eu/activities/studyprogrammes

Better controlling of dissemination activities in FP7

EuresTools Dissemination Tracker launched

Klaas-Pieter Vlieg
Eurescom
vlieg@eurescom.eu

Peter Stollenmayer
Eurescom
stollenmayer@eurescom.eu

Successful dissemination of results by European research projects requires good planning and controlling. Eurescom has made this now easier by launching a dedicated web-based tool for tracking and controlling dissemination activities and outputs. The tool is called EuresTools Dissemination Tracker and is part of the EuresTools suite of modular project management tools.

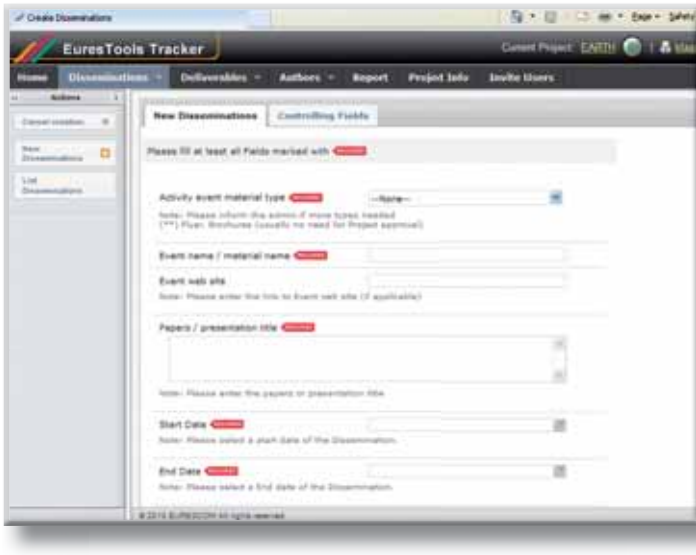
Good project dissemination starts with coordinated planning of dissemination activities, continues with the agreement of the project partners to the content, and culminates in the successful publication, followed by an evaluation of the dissemination impact. In most cases it is not the content of a dissemination activity itself, but rather coordination, information exchange, and agreement between the projects partners on specific dissemination activities, which causes problems.

In addition, professional archiving of all dissemination activities, proper reporting to the European Commission and timely publication on the project website are important and are either forgotten or require significant management effort.

Standard practice is to control dissemination activities with an Excel spreadsheet or something similar. This works to some extent, but requires a lot of manual managerial interventions and many reminders to ensure that all authors enter their dissemination activities. Sometimes important activities are forgotten to be entered and hence do not turn up in reports or on the project website. This is where EuresTools Dissemination Tracker comes into play.

Benefits of the tool

EuresTools Dissemination Tracker is an online tool and can be accessed via any browser by any contributor who is logged into the tool. The tool helps the author to enter the necessary data by providing templates related to the dissemination categories (e.g. deliverable, presentation at a conference, or book article). The author just has to fill in the fields provided by the tool. The fields have been chosen according to the needs of the projects and according to European Commission requirements for reporting. We had many discussions with experienced project managers to ensure that we did not forget any important fields.



How it works

Two different user roles are distinguished in the EuresTools Dissemination Tracker: the Admin and the Author.

Admins can invite Authors, maintain deliverables, control dissemination and deliverable activities, set status and check required field values for each of them and produce reports on these dissemination activities and on the produced deliverables.

Authors can register to the EuresTools Dissemination Tracker after they have received an e-mail invitation, which is triggered by an Admin. They can then submit dissemination activities by filling out a form. The form is well laid out and provides an intuitive interface for entering the essential information related to the dissemination activity, such as the material type, name/title, dates, venue, responsible partner, co-authors, confidentiality level, status, download link, abstract and impact assessment. Co-authors can easily be selected, if their names have been entered before for other dissemination activities.

After submission of a new dissemination activity, an automatic e-mail is triggered to the Admins. This indicates that the project-internal approval procedure for the dissemination activity can start. Automatic reminders can be set to further support this procedure. After project-internal approval or rejection, an automated e-mail is sent to the Author.

Admins and Authors can easily extract standard and customized reports from the EuresTools Dissemination Tracker. These reports can be either in HTML or in various Excel formats. Report definitions can be saved for recurrent usage. Standard reports can immediately be included in reports, e.g. Periodic Report, and are conformant to EC Reporting Guidelines.

Publishing dissemination and deliverable activities to the project website can be done fully automatic. On the relevant web page a reference script can be included which triggers the EuresTools Dissemination Tracker to automatically render the dissemination or deliverable information upon visiting the page.

Conclusion

The EuresTools Dissemination Tracker helps European projects, especially FP7 projects, to control and coordinate their dissemination activities in an efficient way. Agreeing dissemination documents, publishing dissemination documents on the web and preparing proper dissemination activities tables for reports to the European Commission become much easier by using the Dissemination Tracker. Eurescom has successfully tested the tool in ongoing FP7 projects and offers the Dissemination Tracker as an application service provider to any interested project.

You can find more information on the EuresTools Dissemination Tracker at:
www.eurescom.eu/EuresTools/default.asp

An overview on ICT and critical infrastructure protection

Uwe Herzog
Eurescom
herzog@eurescom.eu

We all take it for granted: pressing a switch turns the light on, opening a tap lets the water flow, the heating runs when we wake up in the morning, and our mobile phone keeps us connected and reachable around the clock. We do not think about the critical infrastructures enabling these services, unless they are disrupted. Fortunately, this has happened rarely – so far. However, the risk of more outages is increasing, due to natural and man-made factors, and the effects can be severe, as the recent disaster in Japan has shown.

Modern societies are heavily dependent on the functioning of a number of infrastructures which are, thus, called Critical Infrastructures. They are expected to be available 24 hours a day, 365 days a year. Examples of such infrastructures include ICT, energy and drinking water supply, public health, security services, transport, finance, and some more.

Threats to these infrastructures can have natural causes, e.g. earthquakes, tsunamis, tornadoes, heavy rain, floods, extreme heat periods, or pandemias. On the other hand, risks can also be man-made, caused, for example, by terrorist attacks, online and offline sabotage, maloperation, accidents, or simply system failures. Interestingly, people perceive these risks at very different levels of relevance: risks from terrorism receive often a very high attention by the media and can cause fear, while other risks, like for example failure of technologies or maloperation, are seen as a lesser concern. Due to our extreme dependability on these infrastructures, and due to the strong effects their outages can have, we need to take appropriate measures to protect their operation.

Example: energy supply

Reliable power supply is a basic ingredient of our society. How much this is true we often learn only when there are disruptions. Blackouts have occurred e.g. in 2003 in the US, UK, Switzerland and Italy. A blackout in the Munsterland area in Germany in November 2005 received wide publicity. Nearly 100 powerline poles had collapsed under the heavy snow load and left 250,000 people "power-less" for several days. Only one year later the lights went off in large parts of Western Europe due to an unexpected chain reaction caused by a planned shut down of a high voltage powerline. These examples show the vulnerability in spite of modern technologies employed in material and control. Besides the negative effects on people's daily lives, such blackouts also have huge economical costs: the one-day blackout in the whole north-west of the US in 2003 caused an economic loss of 7 to 10 billion US dollar. Even the blackout in the sparsely populated Munsterland in 2005 caused an estimated damage of about 130 million euro.

Changing general conditions affect ICT

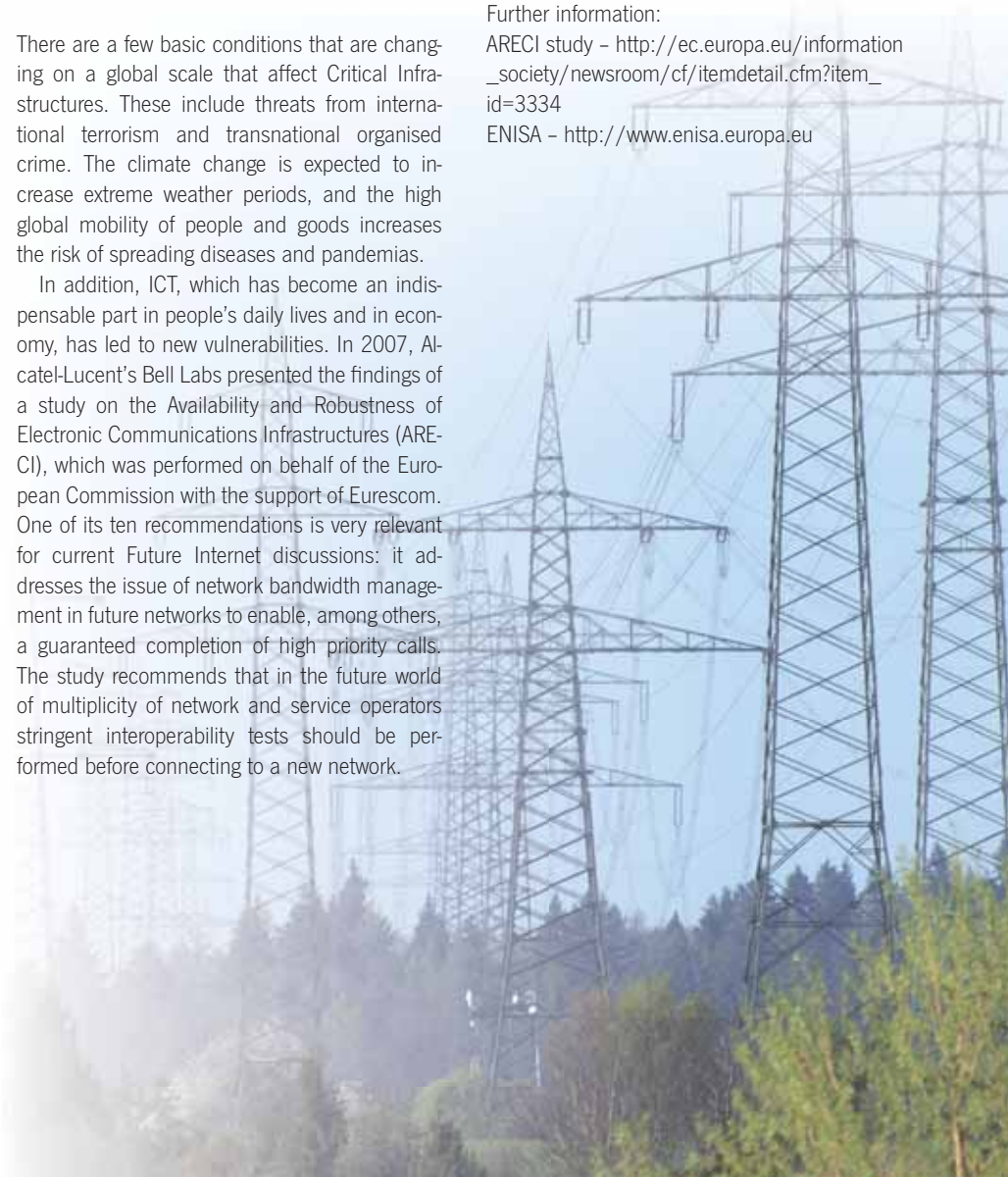
There are a few basic conditions that are changing on a global scale that affect Critical Infrastructures. These include threats from international terrorism and transnational organised crime. The climate change is expected to increase extreme weather periods, and the high global mobility of people and goods increases the risk of spreading diseases and pandemias.

In addition, ICT, which has become an indispensable part in people's daily lives and in economy, has led to new vulnerabilities. In 2007, Alcatel-Lucent's Bell Labs presented the findings of a study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI), which was performed on behalf of the European Commission with the support of Eurescom. One of its ten recommendations is very relevant for current Future Internet discussions: it addresses the issue of network bandwidth management in future networks to enable, among others, a guaranteed completion of high priority calls. The study recommends that in the future world of multiplicity of network and service operators stringent interoperability tests should be performed before connecting to a new network.

Activities at EU level

In 2006, the European Commission released the Directive European Programme for Critical Infrastructure Protection (EPCIP), which was created to identify and protect CIs in EU member states. In the FP7 research programme a joint ICT and Security call for proposals was released in 2007. One of the topics addresses secure and resilient information infrastructures for Critical Infrastructures. Currently, the European Commission together with the European Network and Information Security Agency (ENISA) is establishing a European Public-Private Partnership for Resilience (EP3R). It aims to involve public and private stakeholders in discussions with the goal of strengthening security and resilience in the context of Critical Information Infrastructure Protection. ITU SG 17 is asked to consider the standardisation of the relevant aspects.

Further information:
ARECI study – http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334
ENISA – http://www.enisa.europa.eu



Wireless sensor and actuator networks for critical infrastructure protection

FP7 project WSAN4CIP

Peter Langendoerfer
IHP microelectronics
langendoerfer@ihp-microelectrocnics.com

Wireless Sensor and Actuator Networks are a premium candidate technology when it comes to the challenge of protecting Critical Infrastructures (CI). WSANs can be relatively easily deployed at large scale to cover large geographic areas. As they are normally built from low-cost devices, they provide a very cost-efficient monitoring solution without requiring an additional infrastructure.

In addition, due to the distributed nature and due to the self-configuration capabilities of WSANs, they will even under adverse conditions very likely stay operational, at least on a minimum level. The information that is still harvested and provided will help the CI operator to prevent further damage and to begin the recovery process.

The use of WSANs has significant impact on the dependability of the CI control system and the CI itself. In particular, it is well-known that wireless communication channels are more vulnerable to environmental noise, and hence are in general less reliable than wired links. Moreover, wireless channels are also vulnerable to attacks, such as jamming, injection of forged data and eavesdropping, that are more difficult to carry out in a wired environment, where access to the communication links is physically limited.

Shortcomings of current WSAN technology

Even though the research community has made tremendous achievements within the last years regarding the autonomous, resilient and secure operation of WSANs, a sufficiently high level of dependability of WSANs is still not achieved. In application areas relevant for Critical Infrastructure Protection, wired connections are the reference. Here WSANs have to deal with severe constraints, such as limited resources and publicly shared mediums. In addition, some of the essentially needed core features are still contradictory, for example: strong security and reliable data transfer versus long battery lifetime, or low cost versus stronger processing resources.

In order to resolve these conflicts and to make WSANs a building block for applications that require a high level of dependability, open issues on all protocol layers related to security and reliability have to be investigated. This also holds true for the software deployed on wireless sensor nodes such as operating systems. In addition, designing dependable systems under severe constraints, as it is the case for WSANs, is a highly complex task.

The whole life cycle needs attention

To ensure dependability of WSANs at a degree sufficient for their use as a means for protecting Critical Infrastructures, their complete lifecycle needs to be taken into account, starting with the design phase, including requirements, engineering and determination of its software components via deployment, and normal operations phase.

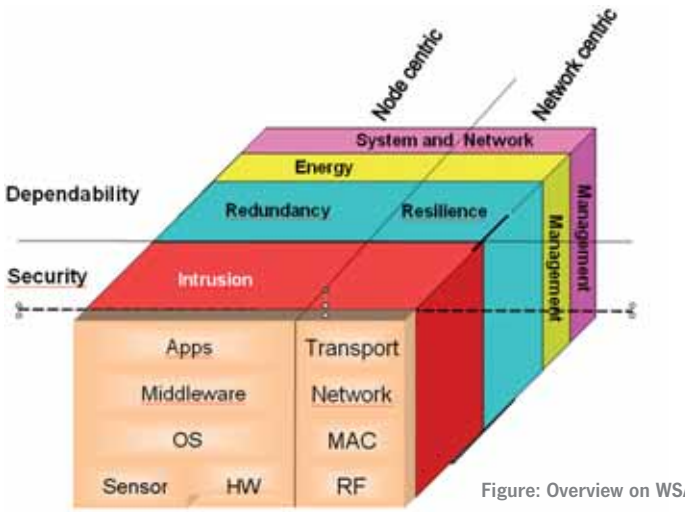


Figure: Overview on WSAN4CIP architecture

EU project WSAN4CIP

In January 2009 the EU FP7 project WSAN4CIP – Wireless Sensor and Actuator Networks for the Protection of Critical Infrastructures – was launched to address current insufficiencies of WSAN technology. The goal of WSAN4CIP is to advance WSAN technology beyond the current state of the art, in order to enable their application for the protection of Critical Infrastructures. WSAN4CIP is a STREP in the ICT security area under Objective 1.7: "Critical Infrastructure Protection". The figure shows the research items that are addressed by WSAN4CIP.

Designing WSANs from an application-centric view

One of the major goals of WSAN4CIP is to provide an application-centric engineering framework for WSAN communication systems. The framework should support system engineers in analysing requirements of the target CIP application and the installation site, e.g. a nuclear power station. We finalized our work on a systematic requirement-driven, tool-supported design flow for WSANs and have implemented a prototype of such a tool. Complementary to that, we specified a simulation environment which can be used to verify dependability properties of network nodes and communication protocols. Moreover, we also analysed network topology issues to increase the resilience of the WSAN. As a result of this work a software tool to compute the strength of given network topologies was developed which can be conveniently used for designing and analysing node deployment strategies.

Protecting the nodes of a WSAN

Concerning the protection of individual nodes, we implemented selected approaches on the hardware platform of a WSAN node. In addition, we designed and implemented a secure key establishment protocol that enables a secure communication between WSAN nodes. The benefit of our approach is that no key distribution is required and that only those two nodes which are willing to communicate are capable to compute the correct key. In order to detect attacks against nodes or parts of the network, a new method called "significance analysis" was researched. First simulations show that it is a promising technology to detect unexpected behaviour. An analysis has shown that the required processing effort

on the node meets the power constraints of a battery-driven sensor node.

Secure software update on the sensor node

It may happen that vulnerabilities or bugs are detected in the software of sensor nodes after their deployment. For this case, WSAN4CIP aims at providing a mechanism for a secure code update in a secure execution environment. In a two-step approach new applications as well as updates are first designed using the tools developed in the project.

Secondly, after the required security level has been verified, software will be deployed using the secure code update, which is almost fully implemented. As a final building block, code attestation techniques to verify the correctness of a deployed system have been researched. The result is a new attestation technique which, however, requires additional hardware for fully secure execution.

Securing the communication between network nodes

The work concerning network protocols focussed on specification and implementation of protocols for all layers. For example, for the network layer, implementations of the two operating systems tinyOS and Linux have already been finalised.

In order to improve the dependability of WSANs, a tool supporting network planning was realised. In addition, new schemes for determining what specific role each respective node in the WSAN should fulfil have been defined. The goal is to hide information on the roles of nodes so that potential attackers are unable to select the most attractive victims, i.e. those nodes which provide a major benefit for the attacker when destroyed or compromised.

Connecting the WSAN with the control system

A WSAN deployed for protecting a Critical Infrastructure needs to be connected to the control system of the CI operator, a system which is called Supervisory Control And Data Acquisition (SCADA). In order to define this interface, a conceptual framework for the design of a SCADA system has been developed. The major innovation achieved by WSAN4CIP is that the framework allows the operator not only to monitor the WSAN but also to give access to the WSAN in order to manage it. This kind of integrated communication network management was not available so far.

Application areas

In order to evaluate our research results, we selected two application areas: energy distribution networks and drinking water supply. Two prototypical demonstrators will be deployed in a part of the power distribution network of EDP Distribuição Energia, a major energy distribution company in Portugal, and in the drinking water network of FWA (Frankfurter Wasser- und Abwassergesellschaft), a regional drinking water and waste water management company in Frankfurt/Oder, Germany.

Conclusion

The field of wireless sensor networks has developed with an exciting pace from pure research to a more or less ready to use technology which is going to be applied in various areas. WSANs will become the glue between a Critical Infrastructure and the ICT Infrastructure which monitors and controls the Critical Infrastructure. A dependable WSAN can keep up the information flow in critical situations, because WSANs are by design fault-tolerant up to a certain level, and thus make the information flow independent of the wired-based control system. WSANs are an ideal technology to inexpensively monitor and manage information about critical infrastructures across large areas.

You can find more information about WSAN4CIP at www.wsan4cip.eu.

Protection of electrical energy distribution infrastructures – The example of EDP

Augusto Casaca
Inesc Inovação
Augusto.Casaca@inesc.pt

Carlos Fortunato
EDP Distribuição
Carlos.Fortunato@edp.pt

The protection of the electrical energy distribution infrastructure is a key task for any operator of such an infrastructure. Securing the main infrastructure components through the deployment of secure wireless sensor and actuator networks (WSAN) that provide remote monitoring and alarm capabilities is an attractive option for achieving this objective.

The European research project WSAN4CIP is searching for innovative solutions for enhancing the reliability and security of critical infrastructures by providing self-healing and dependability modules for WSANs. One of the WSAN4CIP demonstrators is built in the electrical energy distribution network of EDP, the main Portuguese electricity distribution company.

Electricity distribution network

The electrical energy distribution network mainly consists of a set of substations, medium voltage (MV) / low voltage (LV) power transformers, MV power lines connecting substations to MV/LV power transformers and LV power lines from the power transformers to customers. Some industrial customers may also get direct MV power lines. This is illustrated in figure 1. Associated to this network we also consider the Supervisory Control and Data Acquisition (SCADA) system, which is centralized for the whole distribution infrastructure.

Safety and security improvements

For safety reasons, remote surveillance of the electrical energy distribution network is already established to some extent based on wired sensors. The use of WSAN can lead, however, to a more efficient protection of the infrastructure. The higher deployment flexibility allows wireless sensors to capture more status parameters than the existing fixed sensors and can contribute to avoid critical points of failure. Specific actuators can also be included in the infrastructure as part of the WSAN.

For safety improvement, with a direct result in regard to better infrastructure reliability, solutions have been identified for the remote active monitoring of: i) substation circuit breaker trip coil status; ii) substation power transformer oil temperature; iii) substation neutral reactance and neutral resistor coil temperatures; iv) MV power line activity in all three phases to detect location of power line failures; v) remote MV/LV power transformer hotspot detection to detect a likely near future malfunction. All the monitored parameters will be visualized at the SCADA system through a special-purpose interface and a graphical user interface.

Security improvements are focussed on: i) substation perimeter unauthorized intrusion detection by using a combination of cameras, motion detectors and WSAN; ii) intrusion detection in remote MV/LV power transformer installations via deployment of video cameras integrated with the WSAN for image transmission, which get activated by a motion detection sensor.

The WSAN uses Wi-Fi as data link layer communication protocol and includes security features in the network and transport protocols.

Interaction with SCADA

The electricity network devices are nowadays monitored and controlled through the SCADA system. The WSAN will be integrated with this existing system to provide a unified electricity distribution infrastructure interface to the human operators. A high level view is shown in figure 2.

From the supervisor point of view, the SCADA/WSAN gateway behaves as a database that responds to queries about the status of WSAN devices. The application interface for these queries is based on Web Services. From the point of view of the WSAN, the gateway takes the role of the sink node, i.e. it is the destination of all sensed sensor data and the source of queries and configuration/command requests. It also includes a database of sensing and management data.

Conclusion

The electrical energy distribution network constitutes a critical infrastructure in industrially developed societies, which requires protection regarding safety and security threats. The fact that this infrastructure is geographically spread across large areas puts challenges to real-time prevention, detection and precise localization of anomalies and security breaches, which can be significantly improved through the appropriate deployment of secure wireless sensor and actuator networks.

Further information is available at www.wsan-4cip.eu/demonstrators/demonstrator-1-power-distribution.html

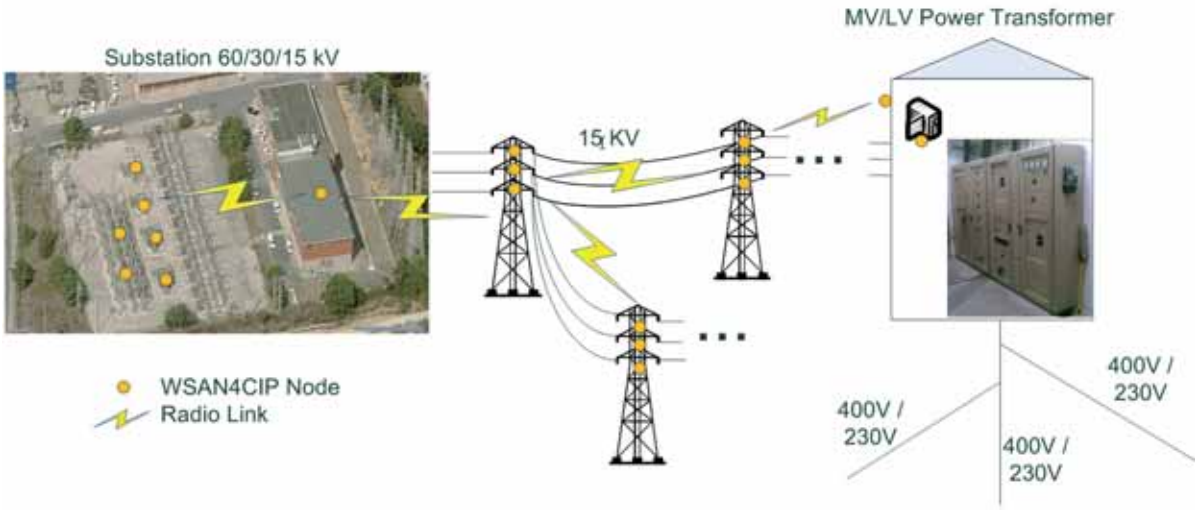


Figure 1: The electricity distribution network of EDP

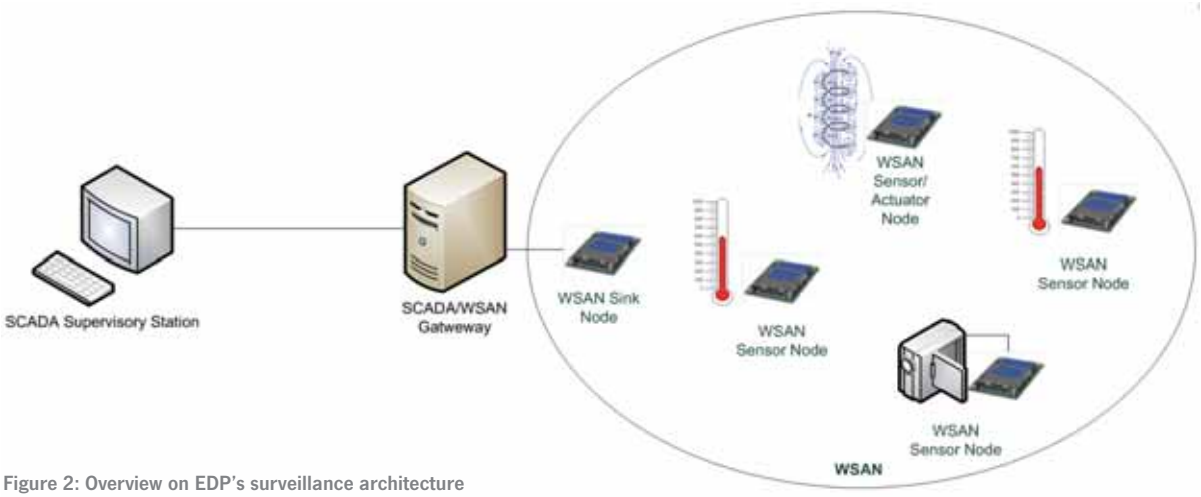


Figure 2: Overview on EDP's surveillance architecture

ICT – The key for successful infrastructure protection

Interview with Aurelio Blanquet from Portuguese electricity operator EDP

One of the most critical infrastructures for the functioning of economy and society is the energy grid. Preventing outages and protecting the energy grid against natural disasters and man-made damages is, thus, one of the central challenges for Europe. This raises the question of how it should be done and which role ICT plays in protecting the energy infrastructure.

Eurescom mess@ge editor-in-chief Milon Gupta asked one of the key responsibles in the European energy sector, Aurelio Blanquet, who is Director for Automation and Telecontrol at Portugal's major energy provider EDP. Energias de Portugal, EDP, ranks among Europe's major electricity operators.

Aurelio Blanquet, EDP

What are the central issues for critical infrastructure protection in the energy sector?

Blanquet: The main issues in the energy sector, from the perspective of EDP Distribuição, are security and reliability. Both are needed for the protection of critical infrastructures. In our case this concerns the energy distribution network and, mainly, the 400 high voltage substations which EDP Distribuição, as Portuguese distribution system operator, is responsible for. In running this infrastructure, cost efficiency is a very important requirement for us. So, what we need for EDP Distribuição are inexpensive and reliable sensors.

How could information and communication technologies help increase the level of infrastructure protection?

Blanquet: ICT is one of the most important vehicles for increasing the level of infrastructure protection, because it may allows sensing in a simple, inexpensive and effective way.

Nowadays, in energy distribution networks, sensing is fundamental for the development of intelligent distribution systems to boost the utility efficiency, increasing the automation of business processes. That's what EDP Distribuição is doing in its Inovgrid project, where we think that wireless technology plays a key role. In fact, this is also why EDP Distribuição is participating in the WSAN4CIP project.

What measures will you take to ensure that EDP's communication channels work in critical situations, like network outages?

Blanquet: Throughout the years EDP Distribuição has developed several initiatives to strengthen its communication network, creating redundancy of telecommunication circuits and using different technological solutions. Sometimes, we have to deal with adverse conditions, mainly wheather-related, and our systems have been very responsive in these cases, proving that we have been doing a good job in the last years.

How will EDP use ICT to tackle current and future challenges for its infrastructure?

Blanquet: At EDP Distribuição we know that ICT is one of the keys for the success of our corporate strategy and business plan.

The market is changing. And EDP Distribuição has a strong commitment to a new sustainable electricity market. This includes integrating distributed energy resources, micro generation and electrical vehicles, increasing end-use energy efficiency, optimal assets exploitation and improving reliability and quality of service.

ICTs have a huge challenge, which includes leveraging the utility strategy through the potential of the technology and in-depth knowledge of the electrical market. It also requires driving the technology evolution and the development of intelligent distribution systems.

Which task do you regard as most important for critical infrastructure protection in the European energy sector in the next five years?

Blanquet: I think that the most important issue for critical infrastructure protection in the energy sector will be Cloud Computing.

In this context, EDP Distribuição is also participating in another European project of the 7th Framework Programme, which is called Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure, short: TCLOUDS. The project goal is to explore the potential of Cloud Computing in critical infrastructures. Security is one of the issues that is not yet very well defined, and so the project will try to give an answer in this area.

Monitoring drinking water pipelines

WSAN demonstrator in Frankfurt/Oder

Steffen Peter
IHP microelectronics
peter@ihp-microelectronics.com

Gerd Weber
FWA mbH
gerd.weber@fwa-ffo.de

Drinking water provision is a critical infrastructure that can benefit from Wireless Sensor and Actuator Networks (WSANs). As part of the WSAN4CIP project, we implemented a demonstrator to prove the feasibility of WSANs. This technology cannot only increase the economic efficiency of the pipeline network, but also improve its safety and security.

Nowadays pipeline networks need to be monitored, in order to ensure the quality of the drinking water and to react quickly in case of accidents, e.g. if pipelines are broken. This type of monitoring is integrated into a Supervisory Control and Data Acquisition (SCADA) management system, operating 24 hours, 7 days a week. In addition, drinking water reservoirs are considered to be also a very sensible part of the network. In the worst case, manipulating the drinking water quality and supply could have immediate impact on the population in the provided area.

The demonstrator is deployed in the waterworks system of FWA (Frankfurter Wasser- und Abwassergesellschaft), the local water provider in the city of Frankfurt/Oder, Germany, about 100 km east of Berlin. The demonstrator monitors the operation of water mains between the waterworks in Briesen and the elevated tank in Rosengarten using a fail-safe and secure data transmission. Between these two facilities, two parallel water pipes run over a total length of 17.5 km. For a primary scenario, data is collected from several pipe access points. The deployed nodes can process the sensed flow rate and pressure measurement data.

Technical realisation

For setting up the demonstrator, each of the access points will be equipped with a sensor node which is able to transmit the sensed data wirelessly. A sensor node consists of a small microcontroller, a radio, and an interface to connect the sensors and actuators. For this demonstrator, the microcontroller is the 16bit TI MSP430, and the radio uses the 868 MHz band, in which sending data is permitted with a power of up to 500 mW. This setup allows wireless transmissions of data for distances of up to 5 km in practice. The node is shown in the figure.

Figure: Node from the FWA water pipeline network

The distance between the furthest nodes and the base station is larger than 5 km. Under bad weather conditions, such as rain or fog, the transmission range can drop to less than 2 km. Thus, it is necessary to send the data hop-by-hop. This means that intermediate nodes have to forward the data packets. However, large distances and several hops increase the possibility of transmission errors significantly.

To cope with those reliability issues, the reliable middleware TinyDSM has been implemented in the project on top of a secure routing and medium access control (MAC) protocol. TinyDSM implements the concept of reliable data storage that helps to assure data availability despite well-known wireless sensor network resource problems. Thereby it adds data redundancy within the network and takes care of the quality of service of the data, e.g. ensuring that alarms are propagated faster than periodic status updates.

Another important requirement for such large networks is the possibility of remote code updates. New node configurations have to be distributed in the network without the need to access each node physically. The FWA demonstrator has integrated a novel secure code update mechanism that not only allows remote configurations but also ensures the correctness of the distributed software.

Conclusion

The novel software modules together with the new sensor nodes promise to fulfil the initial requirements for a secure and cost-efficient wireless surveillance and control network for drinking water pipelines. The practicability of the implementation will be shown in a six-month demonstration starting in summer 2011.

Further information is available at www.wsan-4cip.eu/demonstrators/demonstrator-2-water-distribution.html

Critical infrastructures in emergencies

How to use heterogeneous networks for public safety

Harold Linke
HITEC Luxembourg S.A.
Harold.linke@hitec.lu

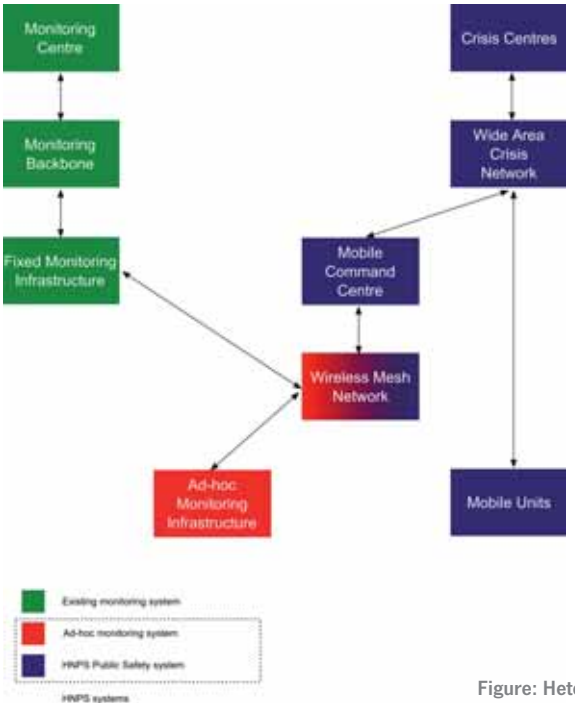


Figure: Heterogeneous network components

The critical infrastructures that support communication have never been more important than in times of a crisis or an emergency. Unfortunately, these are often the same occasions where those infrastructures break down or become unavailable due to physical conditions or excessive demand.

Public safety organisations throughout Europe strive to optimise communication technologies when dealing with emergencies. It is really important that first responders and emergency services have efficient access to all their services (voice and data) through the remaining networks and those quickly deployed by rescue teams.

Objectives

The project HNPS, Heterogeneous Network for European Public Safety, focuses on a well-controlled integration of communication systems, including private mobile radio systems and broadband services, using fixed or deployed networks. This controlled integration leads to the concept of heterogeneous networks for future European public safety communications.

Not only does it allow for the rapid integration of available communication resources but also for the optimisation of rescue resource allocation in order to support the daily operations of public safety agencies. Furthermore it will provide those agencies with a set of advanced digital services that are required for their daily operations.

Approach

The project's approach is based on the use of advanced IP technologies such as IPv6, multicast, network mobility, and wireless mesh networks. It integrates a number of existing and emerging communication systems, e.g. GSM/GPRS, UMTS, TETRA, TETRAPOL, WiMAX, LTE and WLAN. It also includes wireless sensor networks and an experimental wireless mesh network based on the OpenAirInterface platform.

The project establishes an evolutionary approach; the gradual integration of different systems takes the complexity and compatibility of different standards and protocols into consideration. Likewise the system approach is used in application integration and test-bed design. The test bed, developed in the project, created a platform for:

- System compatibility tests, carried out by different research and industrial organisations
- Application integration and interoperability testing
- Usability studies and field trials, with the participation of public safety users
- Training and educational activities

Main Results

The project already demonstrated that its concepts are valid in a simulated scenario that was played out in Paris in November 2010. The scenario showed how different safety and emergency units (personnel including their equipment) could work together, whilst still using different communication solutions, by implementing the project's solutions.

The use of these solutions improved the overall quality of public safety missions. HNPS successfully provided innovative solutions for heterogeneous interworking architectures, adaptive network control and management, interoperable middleware, network cross-layer protocols, ad hoc broadband wireless network protocols, and adaptive applications. Furthermore, HPNS achieved the development of an integrated system for public safety communication. This includes an open interoperable test-bed platform development.

Conclusion

Communication networks of all kinds are available almost everywhere, but nonetheless public safety organisations struggle with interoperability issues and the availability of these critical infrastructures. In the case of a large emergency with many participating organisations and units, it is very likely that these organisations will use different communication technologies as well as services. In a worst case scenario they may not be able to communicate and inter-work.

The HNPS projects demonstrated how the use of heterogeneous networks can bridge those gaps whilst still complementing existing critical infrastructures.

Further information on the HNPS project is available at www.celtic-initiative.org/Projects/Celtic-projects/Call5/HNPS/hnps-default.asp

The new dimension of cyber attacks

Why critical infrastructures need better protection

Heinz Brüggemann
Celtic Office
brueggemann@celticplus.eu

In mid 2010, the computer worm "Stuxnet" infiltrated the control systems of a nuclear uranium enrichment plant in Iran. Only recently it became clear that this highly sophisticated worm was in fact a novel cyber-attack weapon. Reportedly, it destroyed around 1,000 centrifuges, delaying the Iranian nuclear programme by months, if not years. The "success" of Stuxnet, which is said to be already available at the underground community, has further spurred the development of better targeted, smarter and untraceable versions of new "digital explosives".

Worms which directly attack critical infrastructures by trying to destroy sensitive system parts are not completely new. New are the dimensions and the possible degree of devastations and the sophistication of these new weapons. We have to seriously re-think, if all of our critical systems are still sufficiently secured and which additional, even radical, security protection measures we may need to consider.

Rethinking cyber-attack protection

Even the most serious cyber attacks known before Stuxnet, like the distributed denial of service (DDoS) attacks on Estonia in 2007, where nearly the whole banking sector was threatened, had still only a limited potential of real destruction. Despite their economic impact, these attacks were not really threatening whole industries, countries, or large groups of people.

Stuxnet, however, was new and different considering its aggressive destruction potential. The Russian NATO diplomat Dmitry Rogozin recently mentioned that Stuxnet already had the potential to blow up the Iranian nuclear plant in Bushehr – with a chance to cause a second Chernobyl. Are we ready to imagine the impact, if control systems of nuclear power plants, of chemical plants, or of airplanes will be targeted? This could go far beyond the recent concerted computer hacking attacks, which were targeting financial markets and carbon trading registries.

It is estimated that in around 140 countries several hundred thousands of highly skilled experts – in China alone 50,000 to 100,000 – are working on the development of new cyber weapons or the protection against them. If these numbers are correct, it is almost certain that we will soon see many more attacks of much more sophisticated cyber weapons.

We have to be prepared to give up some comfort and commodities, and we have to investigate how vulnerable systems could be better protected.

Consider also radical security solutions

One option to be seriously considered is disconnecting crucial systems from the Net. This sounds like a naïve idea, completely against the current trend of connecting more systems to an even faster Internet. However, experts, like Sandro Gaycken from the University of Stuttgart, promote this idea very strongly. According to Mr Gaycken, we may not have real alternatives to this approach. He said that the US government just released parts of a 'Comprehensive National Cybersecurity Initiative' (CNCI), where plans are described to drastically reduce existing connectivity between state organisations and external networks. Mr Gaycken has no doubts that this will have a serious impact on the functionality and will require a large redesign of complex systems.

Disconnecting critical systems and infrastructures from the Net may not be enough though. Stuxnet infected the system via a prepared USB stick without a connected network. German and British police and security experts are also particularly afraid of internal attackers, people working at the sites and with the targeted systems who have access to infiltrate prepared worms – maybe even unintentionally – via software or firmware "updates". It may, therefore, become necessary to protect the controlling systems from hostile take-over by considering additional means. This could be done by immediately switching a system to an emergency operation mode once unusual system values or behaviours are detected. Updates should always be first tested on stand-by systems before they are installed at the operating systems. We should, however, have no illusions: any system can be compromised. We can only try to make attacks as difficult as possible and stay always vigilant and responsive.

Another option currently discussed is a "kill-switch" for the Internet. It would allow to immediately and widely switch off the Internet in case of massive attacks. However, recent developments during the protests in Egypt and attempts by other authoritarian states raise serious concerns that such a switch could effectively be used also for other purposes to control or prevent information flow between people and turn down riots or unrests.

Conclusion

Even if Europe and many other states have started to develop strategies against severe cyber attacks, the likely dimensions and the urgency for effective and immediately available protection mechanisms may still be underestimated. A lot of effort is currently devoted to design the future, faster, more versatile Internet. Yet it is not fully clear, if really new, far better concepts than today will be considered. They will be a must, as security attacks, including cyber espionage, are increasing to inacceptable numbers.

Providers of services and networks as well as ICT manufacturers should establish closer cooperation activities with the European Network and Information Security Agency (ENISA), which has recently completed its first pan-European cyber security exercise "Cyber Europe 2010" with success. In addition, dedicated research and strategy programmes may be considered that focus on a reliable and flexible protection of the ICT infrastructure against possible cyber attacks.

The next generation of home networking

Final OMEGA Open Event in Rennes

Adam Kapovits
Eurescom
kapovits@eurescom.eu

The third and final OMEGA Open Event in Rennes, France, presented from 23rd to 24th February 2011 leading-edge technologies which will shape the future of home networking. About 100 international experts witnessed the final public demonstration of OMEGA's solutions, which will enable data transmission speeds up to one gigabit per second and the integration of heterogeneous communication technologies in the home.

The 3rd Open Event provided an outlook on the evolution of home networking technologies and made the participants familiar with OMEGA's concepts and technology solutions. In Rennes OMEGA demonstrated its main final results, and participants had the opportunity to get first-hand information about OMEGA's home networking solutions. The Open Event covered the following main topics: connectivity at home, including Radio, Power Line Communication (PLC) and Wireless Optics, as well as the Inter-MAC solution of OMEGA that facilitates the convergence.

Demonstrations

The programme was very much focused on demonstrations and interaction with the audience. OMEGA ran two demonstrations – one showing the power of the proposed Inter-MAC solution through the seamless interoperation of various technologies (power line communication, radio and wireless optics) and one having a specific focus on wireless optics.

The Inter-MAC demonstrator showed, how the Inter-MAC layer enables different use-case scenarios for home networking at gigabit speed. These scenarios included, among others, handover using the best available link, e.g. in case of accidentally broken links, as well as an increase of network capacity and reduced congestion.

Xavier Mongaboure from Spidcom (right) explaining to interested participants OMEGA's results on power-line communications.

Professor Rüdiger Kays (left) from the University of Dortmund and Martial Bellec, technical manager of OMEGA from Orange Labs.

Radio handovers were also demonstrated using a laptop implementing the inter-MAC software developed in the project. Furthermore, OMEGA demonstrated a "follow-me" scenario among two TV sets, using the Inter-MAC layer and UPnP-based session mobility.

OMEGA demonstrated two wireless optics solutions – one based, on infrared and one based on visible-light communication. The infrared demonstrator enables full-duplex communication at 256 Mbit/s in the entire living room, while the visible-light demonstrator enables a 100 Mbit/s broadcast via the ceiling lights – but also through appropriately equipped reading lights – in part of the living room. These demonstrators implemented the full OSI protocol stack, enabling the transmission of live video over wireless optics links.

The audience was able to experience important aspects, such as non-interference between the infrared, the visible-light, as well as radio-based demonstrators and seamless handover when moving a terminal from the area lit by the ceiling light to the proximity of the reading light. The fidelity of both technologies was demonstrated for home-centred use cases, broadcasting high-definition videos in parallel via the ceiling lighting and the infrared demonstrator.

The power-line communication (PLC) demonstrator aimed to show high-bitrate communication up to one Gbps in a PLC environment. The demonstrator emulated the PLC channel model as it was defined in OMEGA, including a PLC channel transfer function and several additive noises in the 0-100 MHz band.

Cyril Bezard from Technicolor explaining and demonstrating the operation of the Inter-MAC.

Plenary sessions

The demonstrations were complemented with interactive plenary sessions. On the first day, OMEGA coordinator Jean-Philippe Javaudin from Orange Labs started with an overview of the project, before OMEGA's technical manager, Martial Bellec, also from Orange Labs, moderated a panel session on OMEGA's challenges and achievements. Topics discussed in the panel session included business aspects of home networking, radio technologies, power-line communication, wireless optics, and Inter-MAC. The panel participants were representatives of major industry players and research organisations from the OMEGA consortium.

On the second day, Rolf Krämer from IHP moderated a panel session on next steps for Inter-MAC, in which the status and perspectives of Inter-MAC were discussed. Prof. Krämer first presented the inter-MAC implementation as shown in the demonstrations. This was followed by a presentation by Paul Houze, chairman of IEEE P1905.1 from Orange Labs, on the Inter-MAC standardisation in IEEE P1905.1. In the ensuing panel session the participants, again representatives of major industry players and research organisations from the OMEGA consortium, discussed how the inter-MAC could be exploited by industry in the home networking eco-system.

Joachim Walewski from Siemens (right) explaining visible-light communication using high-power LED lamps installed in the ceiling.

A terminal unit of the high-speed infrared communication system with transmit and receive sensors and emitters.

Panel discussion on the challenges and achievements of OMEGA (from left): Pierre Jaffré (Orange Labs), Vincenzo Suraci (University of Rome), Joachim Walewski (Siemens), Oliver Hoffmann (University of Dortmund), Dimitris Katsianis (University of Athens), Andrea Tonello (University of Udine)

Tutorials

The programme was rounded off by two tutorials. In the first tutorial, Isabelle Siaud from Orange Labs talked about how to manage multiple radio interfaces in a point-to-point transmission. In the second tutorial, Stefan Nowak from the University of Dortmund explained the Inter-MAC layer and protocols in detail.

About OMEGA

OMEGA is an Integrating Project in the ICT area which receives funding from the European Commission under the Seventh Research Framework Programme (FP7). The project is running for 39 months from January 2008 to March 2011.

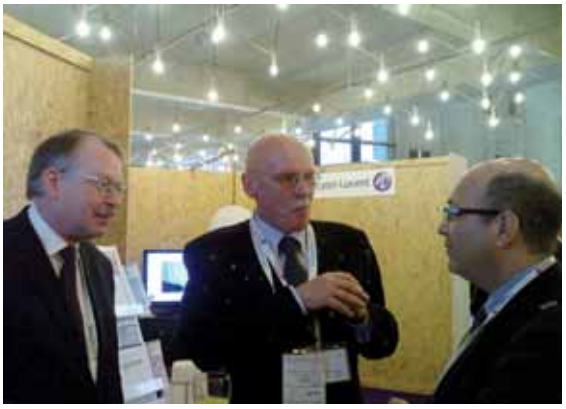
Further information about the Open Event 2011, including downloadable presentation slides, is available at www.ict-omega.eu/events/open-event-2011.html.

eMobility ETP relaunched as Net!Works

eMobility widens its scope and changes name

Net!Works

Uwe Herzog
Eurescom
herzog@eurescom.eu



The European Technology Platform (ETP) eMobility has changed its name and brand to "Net!Works ETP". The main reason for this change was to reflect the extended scope of the platform which now also addresses fixed networks aspects. In addition, the growing use of the term e-mobility in the domain of electric cars seemed to make the name change inevitable.

Background of the relaunch

When eMobility was launched in 2005, the focus of the eMobility ETP was on mobile and wireless communications with an emphasis on the lower network layers. Since then there have been many changes in the ICT sector. Mobile communications, having been in the focus for many years, has become more and more a commodity, and the justification for being treated separately has decreased. Mobility is nowadays just one aspect among many that are relevant for the development of future broadband communications systems in which the border between fixed and mobile continues to blur.

Therefore the eMobility Steering Board already decided in the first half of 2010 to widen the scope of the platform to also address fixed networks aspects. In this context, the platform has established a closer link with the Photonics21 ETP which deals with optical communications. This area is becoming more relevant as the provider of the backbone for broadband systems. In addition, the term e-mobility is increasingly being used in the automotive area when referring to electric vehicles. The eMobility Steering Board has therefore decided to change the platform's name to Net!Works. The new name and white papers with new messages were launched during the Future Internet Week in Ghent from 13-17 December 2010 (see photos).

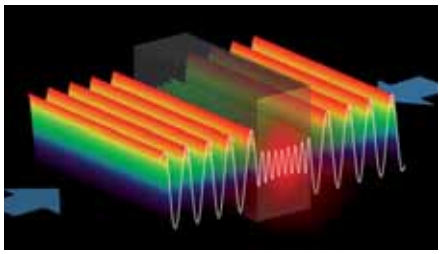
Current activities and plans for 2011

In 2010, the ETP started the discussion on Framework Programme 8 and worked on Grand Societal Challenges. ICT will increasingly be used as a key enabler for other industry sectors and other areas of society. Net!Works will contribute to societal challenges such as energy, climate change, transport, health and the ageing population. Three position papers have been published by Net!Works on its contributions to solving the Grand Societal Challenges. They highlight how Net!Works can help connecting health applications, transport, and the energy and environmental monitoring sectors for a smarter society. The latest version of the Strategic Research and Applications Agenda is a basis for contributing new research challenges. Framework Programme 8 and associated activities will be a major task for 2011.

More information is available on the Net!Works website at: www.networks-etp.eu.

News in brief

Scientists build first anti-laser



Yale University scientists developed the first anti-laser, which allows interfering beams of light to perfectly cancel each other out. (Photo: Yidong Chong / Yale University)

Physicists from Yale University have built the world's first anti-laser. The device can absorb an incoming laser beam almost entirely.

The researchers focused two laser beams with a specific frequency into a cavity containing a silicon wafer that acted as a "loss medium". The wafer aligned the light waves in such a way that they became perfectly trapped, bouncing back and forth indefinitely until they were eventually absorbed and transformed into heat.

The discovery could pave the way for a number of novel technologies with applications in everything from optical computing to radiology. According to Yale physicist A. Douglas Stone, who led the research team, anti-lasers could one day be used as optical switches, detectors and other components in the next generation of computers, called optical computers, which will be powered by light in addition to electrons. Another application might be in radiology, where Stone said the principle of the anti-laser could be employed to target electromagnetic radiation to a small region within normally opaque human tissue, either for therapeutic or imaging purposes.

Theoretically, the CPA should be able to absorb 99.999 percent of the incoming light. Due to experimental limitations, the anti-laser by the Yale researchers absorbs 99.4 percent. Mr Stone, however, is confident that his team will approach the theoretical limit with more sophisticated anti-lasers. The current anti-laser device is about one centimeter across at the moment, but computer simulations have shown that it is possible to build an anti-laser as small as six microns, which is about one-twentieth the width of an average human hair.

http://opac.yale.edu/news/article.aspx?id=8272

EU seeks opinions on e-signatures and electronic identification

The European Commission is conducting a public consultation on e-signatures and electronic identification. Until 15 April 2011, the public is invited to share its views on how e-signatures and electronic identification and authentication could contribute to the development of the European Union's online economy.

According to the consultation website, the purpose of the public consultation is to provide input for policymakers on how electronic identification, authentication and signatures can contribute to deliver the European digital single market. The existing legislation and the established policy landscape, the EC says, are challenged by new factors and technological innovation. In the context of the implementation of the Digital Agenda for Europe this debate is meant to help understand what is needed to create the optimal conditions for their use across the EU.

The consultation process is targeted at key players from civil society, industry, academia and public administrations closely involved in the development and deployment of e-identification, e-authentication and e-signatures. The EC aims to receive their contributions on areas in which the Commission needs to act.

http://ec.europa.eu/yourvoice/ipmforms/dispatch?form=eid4&lang=en

Kroes calls on Member States to act on mobile satellite services

In February 2011, Neelie Kroes, European Commission Vice-President for the Digital Agenda, issued an urgent call to twenty one EU countries to rapidly introduce all the legislative measures necessary to allow the pan-EU deployment of mobile satellite services that could be used for high-speed Internet, mobile television and radio or emergency communications to EU consumers and businesses.

According to the timetable agreed by a Decision of the European Parliament and the EU's Council of Ministers in 2008, mobile satellite services should be deployed in all EU Member States by May 2011 at the latest. In May 2009, the European Commission had selected Inmarsat Ventures Limited and Solaris Mobile Limited to provide pan-European mobile satellite services. However, more than twenty months later, 21 Member States have not yet adopted all the national rules needed to facilitate deployment. Vice-President Kroes also appealed to the two operators concerned to step up their efforts.

Vice-President Kroes particularly urged the twenty one Member States to remove remaining legal uncertainties, such as licence fees, and to put in place all necessary implementation measures without further delay. The twenty one Member States are Belgium, Bulgaria, Cyprus, Czech Republic, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, and the United Kingdom.

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/195&format=HTML&aged=0&language=EN&guiLanguage=en

Digital self-control

How ICTs help resist temptation

Milon Gupta
Eurescom
gupta@eurescom.eu

Many people, including myself, can resist everything except temptation. Almost 120 years after Oscar Wilde coined this famous aphorism, we still find it difficult to contain our cravings for drink, food and some new vices like Internet addiction and compulsive messaging. Information and communication technologies, ICTs, have the potential to equally worsen and improve our addictive behaviour. As ICTs become ever more pervasive, their potential to support us in controlling ourselves is proportionately increasing.

An app for every vice

There is almost no vice, for which ingenious programmers have not developed a self-monitoring application yet. Just look at the plethora of respective mobile apps for iPhone and Android devices. There is for example "Don't Dial!", the app to prevent happy drinkers from making themselves unhappy by calling their boss during a booze. Another one is GlobeTipping, to prevent the over-generous tourist from giving too high tips. Controlling expenses is also the purpose of the Shopulator app, which keeps track of expenses. Those, who like a drink and still want to drive, will appreciate the "Can I Drive Yet?" app, which tells you whether you can still have another drink, before you drive home. This app, however, requires that you remember to enter your drinks correctly, which could become increasingly difficult the more drinks you have.

Blow before you drive

So, to be sure you don't drive when you are drunk requires a more sophisticated application, namely a breath alcohol ignition interlock device. This is basically a breathalyzer hooked up to a motor vehicle's dashboard. Before the vehicle's motor can be started, the driver first must exhale into the device: if the measured breath-alcohol concentration is above the programmed blood alcohol concentration, the device prevents the engine from being started. A number of countries are requiring the ignition interlock as a penalty for drivers convicted of driving under the influence, especially repeat offenders. Some politicians in Sweden, Japan, Canada, the United States and other countries have called for such devices to be installed as standard equipment in all motor vehicles sold.

Less intrusive solutions than the ignition interlock device are currently being developed. The next-generation of alcohol detectors use sensors that measure blood alcohol content either by analysing the driver's breath or through the skin, using sophisticated touch-based sensors placed, for example, on the steering wheel and door locks.

Health monitoring

Sensor-based systems are also the basis for numerous personal health applications. You can measure a wide set of vital functions and provide instant feedback. The earliest example of this in the consumer section have been personal heart rate monitors, which started to be commercially available from 1983 on. With current technologies, the scope of possible applications for health and lifestyle have vastly grown beyond measuring your pulse. Combining today's smart phones with sensors will enable advances forms of monitoring your diet or your stress level and prompt you to take action – "Don't touch this cheese cake!"; "Take a deep breath!". Add accelerometers and GPS to this, and you can monitor practically all human activities and get advice on desirable behaviour. A drinker heading for the next pub would get an alert as soon as he is within 100 meters of the bar.

Negative side-effects

This type of biofeedback offers the opportunity to increase self control and encourage desirable behaviours, like drinking less, eating less, stop smoking cigarettes or overcoming anxiety. However, the constant biofeedback itself could create new anxieties. Getting told to relax and breath deeply when the sensors register increased sweat and faster breathing might not always have the desired affect.

The other important aspect to consider is where ICT-enabled self-control affects human freedom and self-determination. Changing behaviour via biofeedback and conditioning is not new. Since the 1950s, when B.F. Skinner developed behaviourism and promoted the engineering of human behaviour, a fundamental debate has been going on. What are the limits of manipulating human behaviour through technology? Today's technologies allow to improve the behaviour of people, who would not have the self-discipline to eat less, drink less and exercise more with the more or less unobtrusive nudging by caring applications that can replace moms, cops, and doctors at the same time.

The potential of technologies for (self-)control of human behaviours is vast and has not yet been fully exploited. New applications will be invented that can support good social and health-related behaviour. The question we have to ask ourselves is, how much good individual behaviour is good for our society, bearing in mind a thought-provoking aphorism by Henry S. Haskins: "Good behaviour is the last refuge of mediocrity."

EuresTools

Steer your FP7 project to success

The EuresTools suite of project management tools has already helped more than 120 European research projects to be efficient and successful.
EuresTools enables coordinators of FP7 projects to effectively manage reporting, dissemination, and project-internal communication. All project partners benefit from EuresTools via easy reporting and effective virtual-team communication.

What's best: you can get EuresTools fully funded by the EC, if you include it in the budget of your project proposal.

Benefits of EuresTools include:

- **Fast and simple project reporting**
- **Effective document sharing with versioning and change tracking**
- **Smooth project-internal communication via mailing-lists, audio- and web-conferencing**
- **Semi-automated dissemination and deliverable tracking**

Contact us to get more information and a live demonstration via EuresTools Web Conferencing – e-mail: services@eurescom.eu.

www.eurescom.eu/EuresTools

EURESCOM mess@ge

The magazine for telecom insiders

Get your free subscription of Eurescom mess@ge at www.eurescom.eu/message

EURESCOM

European Institute for Research
and Strategic Studies
in Telecommunications GmbH
Wieblinger Weg 19/4
69123 Heidelberg, Germany
Tel.: +49 6221 989-0
Fax: +49 6221 989 209
E-mail: info@eurescom.eu
Website: www.eurescom.eu

20 Years of Innovation through Collaboration

Eurescom is the leading organisation for managing collaborative R&D in telecommunications. Our mission is to provide efficient management and support of R&D projects, programmes, and initiatives for our customers. We offer 20 years of experience in managing large-scale, international R&D for major industry players, the European Commission, and EUREKA Cluster Celtic-Plus. What distinguishes Eurescom is the combination of a secure, reliable infrastructure for collaborative work, a large European network of experts, and internationally outstanding project management skills.

QR code to the online edition of Eurescom mess@ge