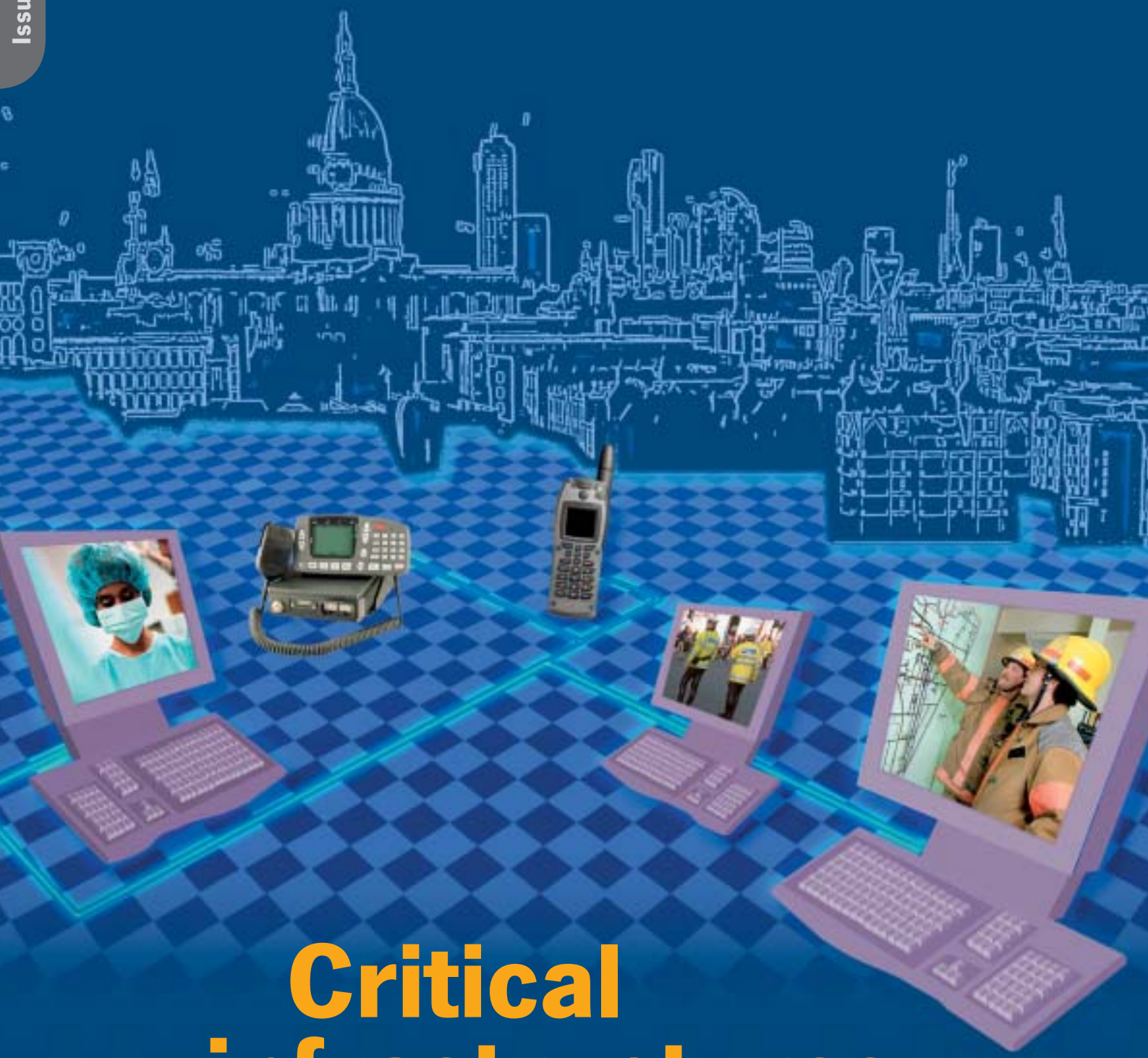
EURESCOM mess@ge
Issue 3/2004



Critical infrastructures

In focus
Wireless World Research Forum

Tutorial
ENUM

Project reports
European security research

Call for Papers

Eurescom Summit 2005
27-29 April 2005
Heidelberg, Germany

Ubiquitous Services and Applications
Exploiting the Potential

SCOPE

The continuing evolution of telecommunications and information services is delivering the technology to fulfil the promise of omnipresent services and applications. Pervasive computing and ubiquitous services, which facilitate the users' everyday activities, have been an intense research issue over the last years. Today, many technologies are available that can be combined to exploit the business potentials of services and applications which work anytime and anywhere in a seamless and intuitive way.

The fourth Eurescom Summit focuses on 'Ubiquitous Services and Applications'. The conference aims at investigating technical issues of ubiquitous services, showing how the advances in enabling technologies can support the exploitation of ubiquity. The conference will also consider the exploitation opportunities, usability and user acceptance, and will evaluate their business relevance.

Authors are invited to submit papers addressing, but not limited to, the following topics:

- Evolution of ubiquitous services and applications
- Service platforms, systems & architecture aspects
- Business aspects, opportunities and threats
- User aspects, acceptance, privacy
- Technology aspects, devices
- Content related aspects
- Self-organisation/self-configuration of networks
- Security aspects

A more comprehensive list of topics is available on the conference website.

ENDORSED BY

INFORMATION FOR AUTHORS

Submissions should be 800-1500 words abstracts summarising original work. It must be clear from the abstract how it is going to be extended to a full paper. All manuscripts must be written in English. The first page of each paper should contain: the title of the paper, the name(s) and affiliation of the author(s) as well as full address, e-mail and phone number of the author responsible for correspondence.

The selected papers will be published in printed proceedings with an ISBN. Papers must be submitted electronically via the conference website. A document template and further instructions for paper submissions can be found on the conference website.

IMPORTANT DATES

- 15 October 2004
  Submission of 800-1500 words abstracts (2 to 3 pages)
- 15 December 2004
  Notification of authors
- 21 January 2005
  Final camera-ready papers (max 8 pages or 4000 words)

CONFERENCE WEBSITE AND FURTHER INFORMATION

Further information can be found on the Eurescom Summit 2005 website http://www.eurescom.de/summit2005 or through the following contacts:

E-mail: summit2005@eurescom.de
Tel: +49 6221 989-0, Fax: +49 6221 989 209

POSTAL ADDRESS

Eurescom GmbH
Schloss-Wolfsbrunnenweg 35
69118 Heidelberg
Germany

www.eurescom.de/summit2005

The enlargement of European research

Dr. Claudio Carrelli
Eurescom
carrelli@eurescom.de

The enlargement of the European Union has changed the political and economic landscape in Europe. It has also changed the landscape of European telecommunications. Although the economic weight of the ten new member states is still relatively low compared to the fifteen old member states, the telecoms sector is growing fast, especially in the Central and Eastern European member states.

According to the last EITO report, the combined Western European and Central and Eastern European telecommunications markets have a size of over 300 billion euro. Market analysts predict a two-digit growth of this figure, as a combination of new fixed and mobile access products emerge on the market. The growth of Central and Eastern European markets is mainly due to mobile as well as Internet and data services. End users increasingly rely on mobile phones for not only voice calls but also other types of telecommunications, like data transfer and Internet access. As these markets are far from being mature, they will offer considerable growth opportunities over the next few years.

In addition to the telecoms market opportunities, the new member states, especially in Central and Eastern Europe, have more to offer. There is a large, well-educated work force in these countries, which has already contributed to increasing Europe's competitiveness in telecoms. Manufacturers like Siemens, Alcatel, and Ericsson have been actively tapping this human potential, as did network operators like Deutsche Telekom who acquired shares of telcos in those countries.

In this context, it has to be stressed that the new member states also offer a large potential of researchers in the ICT domain. In countries like Poland, Hungary, the Czech Republic, the Slovak Republic, and Slovenia, there have been traditionally strong ICT research institutions with a number of qualified researchers, and also the Baltic states, Cyprus, and Malta have their resources. This research potential has so far only been used to a limited extent.

Within the EU Framework Programme 6, the new member states have been clearly under-represented. Their integration into the emerging European Research Area has been poor. A number of factors within the countries have led to this situation: insufficient knowledge about the mechanisms of EU programmes, lack of language capabilities, lack of contacts to Western European partners. The European Commission has added to these structural problems by failing to provide enough specific information to potential project participants in the new member states that would facilitate their involvement.

The European Commission is aware of these problems and has taken countermeasures, for example by specifically addressing the current third call of FP6 to the needs of the new member states. Helping the new member states to get connected to European ICT research activities is in the interest of Europe's economic position in the world. It is more than just providing development aid to economic laggards. In fact, countries like Estonia are already more advanced in terms of mobile phone usage penetration than most of the old EU member states. The lack of a good legacy fixed-line network has been an incentive in the new member states to implement innovative solutions, especially in mobile networks. Thus, the new member states could offer innovation laboratories with a precursor function for other European countries.

What is even more important is that Europe needs to mobilise all intellectual capacities in order to sustain and improve its competitive position in the world. Apart from better involving experienced telecoms experts from the new member states in European research projects this would also include a more pan-European approach to education in the relevant engineering sciences. If this is not done, we might have to face a heavy brain drain from new member states. Ivan Wilhelm, Rector of Charles University in Prague, regards such a "brain drain" from Eastern and Central Europe as a "very real possibility", because of more attractive salaries and more attractive job conditions in other EU countries. To counter this trend, which could slow down economic development in the new member states, he called on the EU to "implement a strategy in order to change the situation very quickly and create as homogenous a European Research Area as possible". If the brain drain just took place within Europe, this might happen without negative effects on the overall research capacity. However, there is the serious threat that talented engineers from the new member states wouldn't stop at the EU borders, but would move across the Atlantic.

Public and private efforts for building the European Research Area could prevent this brain drain and best utilise the intellectual potential we have in an enlarged Europe for developing a leading knowledge economy in Europe.

Eurescom has supported pan-European research since it was founded in 1991. Among the members of Eurescom are Hungarian network operator Matáv, Slovak Telecom, Cyprus Telecommunications Authority (CYTA), and Yugoslav PTT. In addition, Eurescom's EU projects involve a number of partners from the new member states.

In conclusion, FP6 and Eurescom offer the opportunities for integrating the new member states in public and private European ICT research. It is now upon the relevant players in the new member states to grasp these opportunities for collaboration.

Dear readers,

While this issue of *Eurescom mess@ge* was edited, the Olympic games in Athens were in full swing. There was plenty of media coverage on the security efforts to protect the sites of the games from terrorist attacks. An aspect which did not catch the attention of the media was the huge challenge the Greek communication infrastructure faced because of the games, even without the Damokles' sword of terrorist attacks. This event and new research results triggered our decision to focus on critical telecommunication infrastructures in the cover theme of this issue.

Our authors may be less known to the world than the Olympic athletes from Athens, but their expertise and importance in regard to the cover theme is of Olympic dimensions.

Luis Cardoso, chairman of the ETNO working group on Fraud Control and Network Security from Portugal Telecom, gives an overview on Internet infrastructure and fraud. Two experts from the EU CGALIES working group present in an interview the state of the art regarding the enhanced 112 European emergency call. In another interview, the CEO of the TETRA MoU Association, John Cox, reveals important facts on secure communication systems.

Related to our cover theme are the two articles under "European issues". In the first, we feature the new European Network and Information Security Agency, ENISA, and in the second we present an overview on European security research.

In our "In focus" section, we present for the first time not a member company of Eurescom but an international organisation, which is relatively young, but highly influential: the Wireless World Research Forum (WWRF).

The further content of this issue includes contributions on Eurescom study NEMOGS and Eurescom project GENIE, a tutorial on ENUM, and the "A bit beyond article" on stealth wallpaper.

We hope you will find something interesting in this issue and would appreciate your feedback on any of the articles. If you would like to suggest a topic or offer a contribution for *Eurescom mess@ge*, this is equally welcome.

Enjoy reading this issue.

Your
mess@ge editorial team
message@eurescom.de

Sn@pshot

Mobile phone throwing – soon Olympic?

Selecting the right piece of sports equipment is crucial.

Junior contestant in deep concentration before her throw.

Young mobile phone thrower in full action.

Photos from the fifth Mobile Phone Throwing World Championships in Savonlinna, Finland, 28th August 2004.
New world champion is Ville Piippo from Helsinki, who threw a Nokia phone 82,55 metres.

INTRODUCTION
The enlargement of European research 3

EDITORIAL REMARK 4
SN@PSHOT 4
NEWS IN BRIEF 6

COVER THEME

Critical infrastructures

An introduction to critical infrastructures 7
Internet security and critical infrastructures 8
Location-enhanced 112 in Europe – interview 9
The role of OSS in protecting the network 10
Milliseconds are vital – interview 11
TETRA and TETRAPOL 11

IN FOCUS
Wireless World Research Forum (WWRF) 12

EVENTS
SOCQUIT Seminar – IST and Quality of Life 14

PROJECT REPORTS
NEMOGS – GALILEO satellite services 15
GENIE – GMPLS and MPLS in Enhanced IP Networks 17

TUTORIAL
ENUM – The bridge between telephony and Internet 19

INTERNAL
France Télécom takes the chairmanship 21
Fireworks – Interconnection of multimedia services 22
New Eurescom studies – WiBAN 22

EUROPEAN ISSUES
ENISA – New agency for network and information security 23
The European Security Research Programme 24

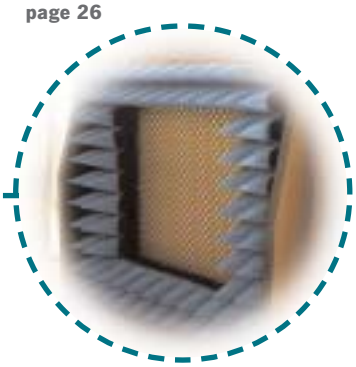
NEW PROJECT RESULTS 25

A BIT BEYOND
Stealthy wallpaper 26

Critical infrastructures
page 7

Wireless World Research Forum (WWRF)
page 12

New ideas for your interior design – stealthy wallpaper
page 26



Imprint
EURESCOM mess@ge, issue 3/2004 (September 2004)
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 · Schloss-Wolfsbrunnenweg 35 · 69118 Heidelberg, Germany
Tel.: + 49 6221 989 – 123 · Fax: + 49 6221 989 – 209 · E-mail: message@eurescom.de

Advertising: Luitgard Hauer, phone: +49 6221 989 – 405, e-mail: hauer@eurescom.de
Distribution: Eurescom mess@ge is distributed quarterly.

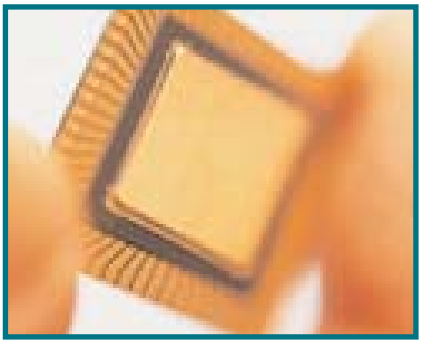
Eurescom mess@ge on the Web:
http://www.eurescom.de/message

+++ News in brief +++ News in brief +++

China developed first home-grown 3G mobile phone chip

China has successfully developed an own 3G mobile phone chip, as reported by Chinese news agency Xinhua. The Chinese mobile phone chipset was developed by the Shanghai branch of Spreadtrum Communications Inc., a provider of wireless integrated circuits software solutions. According to a report in the online news portal "The Register", much of the engineering for the chip was carried out by Spreadtrum's Sunnyvale headquarters in California's Silicon Valley. Part of the development cost was financed by the Chinese Ministry of Information Industry, MII.

Spreadtrum claims that major Chinese mobile phone manufacturers like Amoi, Bird, Lenovo, and Hisense have already agreed to use the Chinese 3G chip. Currently, Chinese mobile phone manufacturers pay more than 10 billion US dollars for imported chipsets. This is due to a market price of 25 to 50 US dollars for a single chipset, which makes up 50 to 70 percent of the cost of the phones, according to Xinhua.



The development of a Chinese chip is expected to decrease the dependency of Chinese mobile phone makers on foreign intellectual property and significantly lower the amount of license fees paid to foreign chip makers. This will have a significant economic impact, as China's mobile phone market is the biggest in the world. At the end of July, the number of mobile phone users hit the mark of 310 million.

The launch of 3G in China has been repeatedly postponed. The Chinese government has been testing all three available standards: WCDMA (UMTS), the US standard CDMA 2000, and the Chinese standard TD-SCDMA. According to a report on news portal Heise.de, the government promotes the Chinese standard, but allows service providers to choose their preferred standard.

www.spreadtrum.com
www.mii.gov.cn

France Télécom and Deutsche Telekom agree on R&D cooperation

France Télécom and Deutsche Telekom have agreed to cooperate in selected areas of innovation and R&D. On 15 July, the CEOs of France Télécom and Deutsche Telekom, Thierry Breton and Kai-Uwe Ricke, signed a Memorandum of Understanding (MoU) to this effect in Paris. France Télécom and Deutsche Telekom aim to develop future-oriented applications and services for next-generation networks and for intelligent access technology in future.

Cooperating: Kai-Uwe Ricke (left) and Thierry Breton

Thierry Breton, CEO of France Télécom, said: "Innovation is a key driver for sustainable growth for operators in the communication sector; partnership in innovation between global operators as France Télécom and Deutsche Telekom will accelerate the development of the communication market in Europe, putting our customers at the center of their communication network."

Kai-Uwe Ricke, CEO of Deutsche Telekom, emphasized: "By working together in research and development projects, Deutsche Telekom and France Télécom want to play an active role in shaping the telecommunications market of the future."

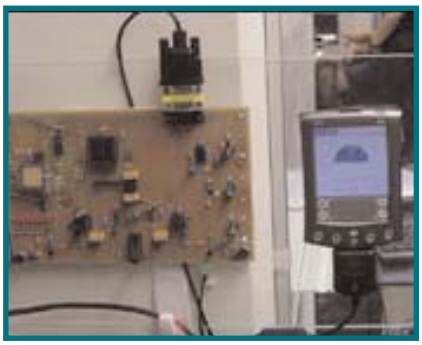
This cooperation aims to strengthen Europe's position in global ICT. In this respect, both operators declared to be open to other partners in developing their R&D collaboration. By performing shared applied research and joint technology projects, France Télécom and Deutsche Telekom aim to deliver to their customers a higher quality of services at reasonable cost.

By developing joint positions in standardisation, both companies will ensure international interoperability of devices and services. The cooperation will focus mainly on next-generation networks, cross-network customer access, service delivery platforms, terminal devices of the future, and the home gateway.

www.telekom3.de
www.francetelecom.fr

Mobile telephony: dual microphone against background noise

Scientists at the University of Toronto have developed an innovative speech recognition system for reducing background noise. Parham Aarabi and Guangji Shi designed a signal enhancement algorithm that employs two microphones and a number of filters. A computer chip analyses the amount of time it takes for sounds to arrive at the two microphones. Thus, the chip determines which signals arise from a speaker and which come from other sound sources.



The new approach has improved on the performance of alternative speech recognition systems by about 30 percent, the researchers report in the August issue of the journal "IEEE Transactions on Systems, Man, and Cybernetics" (part B). "Other speech recognition systems only reduce the background noise, but this technology also deconstructs other conversations into a slight hum so they don't confuse you," Aarabi explained. The team hopes to have customized chips that can be used to enhance computer voice recognition software ready in the coming months. Cell phone users will have to wait a few years before the technology is small enough to carry with them, however. The novel dual microphone system could be miniaturised within two years, according to Aarabi and Guangji.

www.comm.toronto.edu/flabs.html

An introduction to critical infrastructures

Anastasius Gavras
Eurescom
gavras@eurescom.de

Modern life has become dependent on several services and facilities that we take for granted. We take the availability of electricity and water supply as well as the existence of transportation and telephone systems as given. It is not easy to define the term "infrastructure" in the context of the dependency of modern life on it. Even more difficult is the definition of what constitutes a critical infrastructure.

The notion of criticality depends on the standpoint. A government has different priorities for classifying infrastructure as critical than an organization or an individual. Typically, in the civic sense infrastructure includes (a) transportation, e.g. roads, railways, airports, (b) utilities, e.g. electricity, water supply, sewers, telephone, broadcast, and (c) municipal services, e.g. police, fire protection, refuse collection.

At the government level the term "critical infrastructure" is very broad, although it should be less inclusive as not all infrastructure should be considered critical. In some definitions it even includes support, e.g. for banking, and other such processes not necessarily critical to survival. One issue is the necessity of means of protection in increasing the quality of life. Another issue is whether means of persuasion, like computer or broadcast technology, can qualify as infrastructure in any sense, as it is more belief-sustaining than life-sustaining. A more narrow definition would include only the services and facilities whose protection, especially in emergency response, is critical to survival.

Classifying criticality

Criteria for classifying a facility or service as critical infrastructure have evolved over time. For an infrastructure to be judged critical it must be vital to one or more broad governmental functions. This set of functions has expanded over time, including national defence and economic security as well as public health and safety. In order to classify their criticality, the sectors are identified and assessed with respect to the functions. Telecommunications and information networks, for example, can be classified as critical for the national defence and economic security.

Interdependencies

A number of facilities and services depend on each other. Airports and railways depend on electricity and communications. The power grid itself depends on communication among power plants and distribution nodes, and the telecommunications network depends on power supply for the transmission links and the exchange nodes. Analysing the infrastructures and their interdependencies one will soon discover that the telecommunications and information networks, together with energy, are at the heart of almost all other infrastructures. This is reason enough for this issue of *Eurescom mess@ge* to address the critical dependency of our quality of life on the telecommunications and information networks.

The article on "Internet security and critical infrastructures" by Luis Cardoso provides an overview on the issues involved in network security and its important role for enabling the information society. In particular, the security of the networks is a prerequisite for building confidence in users.

The network operation support system (OSS) has long been recognised as a critical business success factor for telecommunication operators and service providers. Furthermore, the OSS contributes and supports the critical infrastructure of the information society as well. The further development of OSS interconnection standards will take into account the need for interchange of critical network and service management information between service providers. This exchange requires cooperation at the international level, a fact that has been recognised at the relevant standardisation bodies.

Other contributions of communication technologies to public safety and disaster relief in Europe are the two major radio systems TETRA and TETRAPOL, which have been specifically designed for reliable use during incidents. Both systems are standardised and supported by international telecommunications standards bodies.

At the European Union level

The establishment of emergency services like police and fire department is a major achievement of civilisation. In case of emergency the network infrastructure will support the dispatch of an emergency call to the right service. The requirements on the availability of such services are very high. At European level, the unified emergency calling number 112 is operational in all counties. The next step is the location-enhanced 112 service. This service might prove vital in the case of a car accident in a remote area. Even if you might be able to call 112 from your mobile phone, you might not be in the mental or physical position to specify exactly the location of the accident. The location-enhanced 112 service will close this gap.

In the context of efforts to protect critical infrastructures, the new European Network and Information Security Agency, ENISA, has to be mentioned. ENISA was set up in March 2004 and is expected to become fully operational in autumn 2004 with the nomination of its executive director. Its primary objective is to enhance the capability of member states and companies in the European Union to prevent, address and respond to network and information security incidents. However, the security challenges go much further.

One of the fundamental roles of government is to help ensure the security and quality of life of its citizens. Studies show that the threats of terrorism, organised crime, and natural disasters are among Europeans' worst fears. Making Europe more secure for its citizens while increasing its industrial competitiveness is the goal of European security research. The European Commission has recently launched a preparatory action on "Enhancement of the European industrial potential in the field of Security Research 2004-2006" for addressing key security challenges facing Europe and its partners. The report of the Group of Personalities, which preceded the launch, identifies, among other areas, security against cyber-attacks, secure digital communications, and many other network related aspects as fundamental capabilities of critical infrastructures.

In conclusion, the telecommunication and information network infrastructure has become a vital element enabling our quality of life as well as a key aspect in the mission to protect us from various threats. We are not only exploiting the benefits of the technologies, but have also recognised the urgent need to develop coherent European strategies to protect our critical infrastructure.

Internet security and critical infrastructures

Luis S. Cardoso
Portugal Telecom
luis-s.cardoso@
telecom.pt

One of the enabling elements to create an information society in Europe is fast and secure Internet. The security of electronic networks and information systems is a critical issue for the use of new technologies in all fields of life, and in particular in e-commerce. It is a prerequisite for building confidence in users.

Internet and network infrastructure

The definition of network infrastructure is dependent on the context in which it is used. A network infrastructure can be identified as a public or private network that carries information of high financial value or information relevant to national security and safety. Network infrastructure can also be defined physically as the whole network or a part of the network that exchanges information of high significance. For example, if the objective of the network itself is to exchange confidential information among nations, the whole network itself can be defined as a network infrastructure. However, in the case of the Internet, it is appropriate to define pertinent parts as network infrastructures, because its objective is to simultaneously share information that is open to many anonymous users, and it has been increasingly used as a means to exchange information which is important for society and the economy.

While communication networks have become an ever-increasing part of our daily lives, so does our dependency upon their underlying infrastructure. Unfortunately, as our dependency has grown, also hostile attacks on the infrastructure by network predators have increased in number and impact. Newly discovered forms of attacks, the availability and wide distribution of attack tools, as well as the flaws in common desktop software have resulted in networks becoming increasingly vulnerable. Sophisticated, distributed denial-of-service attacks on the Internet are rising, and simple viruses are argued to have cost billions of dollars worldwide in lost productivity.

For these reasons, it is essential to guarantee the security of information which is considered of critical importance, from a political, economic, financial or social standpoint. In order to safeguard critical information resources and to guarantee network security, the technical aspects of network security have been explored in many studies. Even if large parts of the network have state-of-the-art security, in practice the level of security is only as strong as the weakest link in the entire network.

Current information security services, which are used in individual systems, are generally limited by regulations and legislation to national borders, rather than being applied to all nations or to international networks. Since the security system is usually located at the network access point, it is imperative to have a security plan for the access point. In addition, interoperability among individual security systems must be provided and security nodes must be monitored and controlled. Furthermore, secure network techniques should be introduced in order to provide information security services which meet diverse user requirements. Only a combination of measures can result in improved protection of critical network infrastructures.

Effects of network vulnerabilities

There are several examples of damage that may result from vulnerabilities or defects in today's network infrastructures. Services with high financial value, such as banking, e-commerce, and trade, exchange confidential data worldwide, beyond the boundaries of national network regulation and legislation. Other industries, such as aviation, space transport, mass transit, and shipping, also depend on the network infrastructure. Elements of a transportation system, such as communication, navigation or the information network, can be threatened in numerous ways. For instance, there are only few technical security features implemented in the GPS (global positioning system), which is used as a navigation tool for aircraft, ships, and automobiles as well as a positioning tool during military operations. Power supply can also affect the physical aspects of network infrastructures. Natural disasters can damage important data even if perfect back-up systems are available. Other examples of dependent infrastructures include energy infrastructures, such as oil and natural gas. Similarly, cyber disruptions can result in damages of these infrastructures stretching over a wide geographical range. A reliable international security system is necessary, if such damage is to be prevented in advance.

Impact of new technologies

There are also new security threats in telecommunications resulting from the evolution of cellular and other wireless technologies. Cellular devices, in particular, are becoming general-purpose computing platforms. These devices are present in very large numbers, and most are supported by software provided by a small number of manufacturers. These manufacturers' operating systems, now somewhat obscure, are becoming familiar to attackers.

The increasing prevalence of Internet connectivity in wireless networks opens these devices to the same avenues of attack as currently available for non-mobile Internet hosts. In addition, device mobility complicates the auditing and control of device configurations. The cellular infrastructure could be especially vulnerable to phone-based threats, especially if Internet access is provided via an internal network, logically located inside the carrier's network.

Raised awareness

Network infrastructure security has become a high priority issue due to a variety of reasons, including data protection, economic dependency, national security, and e-commerce. These are good reasons for international cooperation. Currently, although each country applies legal restrictions for network infrastructure security based on its own network situation, there is no international legal policy or system that applies. A systematic international legal solution for network infrastructure security must be developed. In the past few years, there has been an increase in the number of infrastructure security initiatives around the world, as a reaction to many and varied network security incidents. In Europe a new agency, ENISA, is becoming operational, which will address some of the issues. Among the European standards organisation, a new group has been set up to co-ordinate security issues.

Conclusion

The knowledge on computer security has already reached a high level, but the implementation lags far behind, with continued failure to implement security measures. There are a number of reasons for this deficit. Information on the details of security vulnerabilities, threats, and breaches is insufficient, and incentives to encourage the private sector to improve critical infrastructure protection are lacking. This is exacerbated by technology and competition cycles, which provide further disincentives for the private sector to pay attention to and invest in critical infrastructure protection. Better data will certainly help, because it will demonstrate the case for improved critical infrastructure protection. The establishment of an incentive structure, which might include insurance requirements, liability, standards, and R&D and tax credits, should accompany this.

At EU level, from a policy standpoint, both the improvement of technologies for e-procurement and the reform of existing

public procurement procedures are now regarded as complementary measures that will enable public utilities and other public sector organisations in the EU to make more extensive use of public procurement as an instrument for stimulating private sector research and development. However, such public services can only be developed, if trust in the network infrastructure and service security can be increased.

Further information about INNO-UTILITIES is available at www.inno-utilities.org

Location-enhanced 112 in Europe

Interview with emergency-service experts Knut Viddal-Ervik from Telenor and John Medland (BT)

Knut Viddal-Ervik

The availability of a location-enhanced, unified emergency call number has been made a goal of high priority by the European Commission. In July 2003, the Commission issued a Recommendation for the Europe-wide implementation of the location-enhanced 112. From 2000 to 2002 the Coordination Group on Access to Location Information by Emergency Services (CGALIES), which was established by the Commission, explored what has to be done to achieve this. *Eurescom mess@ge* talked to emergency-service experts Knut Viddal-Ervik and John Medland, who were both members of the CGALIES working group. Mr Viddal-Ervik is Product Manager for Emergency Services in Telenor and a member of the ETSI OCG EMTEL working group, Mr Medland is "BT 112 and 999 Product Manager".

What is the current status of implementing location-enhanced emergency call services in Europe and especially in Norway?

Viddal-Ervik: Enhanced location information for emergency services is available today from most mobile operators in Norway. The Norwegian legislation has been updated as from 1st July 2003.

For the fixed network there is still some work to be done. Telenor and a couple of other telcos in Norway do provide such information; others do not. The regulatory body in Norway will put pressure on the telcos that do not provide such information.

Medland: In the UK, both fixed and mobile locations are automatically available over a separate data link to the emergency services as soon as they answer the 112 call. At present, about one third of UK emergency services, or second stage PSAPs (Public Safety Answering Points – the editor), use this facility, provided by first stage PSAP, BT, that answers 80% of UK 112/999 calls.

What is yet to be done to make the location-enhanced 112 happen?

Medland: In the UK, more local emergency services need to make use of the information provided by the telecommunication companies. This includes the separate fire, police, ambulance and coastguard services.

Viddal-Ervik: The PSAPs must buy the location information from mobile phones on a commercial basis. Many PSAPs have not done this despite this has been demanded for years. Mobile providers have informed the PSAPs about the availability. The large PSAPs have implemented the service.

Where are the challenges in the implementation process?

Viddal-Ervik: The biggest challenge in Norway is for the PSAPs and telcos to agree upon a standard to be used. Telenor has provided location information in the fixed network for years, and the PSAPs are familiar with this standard. A lot of other telcos in Norway are reluctant to use Telenor's system and have demanded that another standard should be developed and used. This standard is not complete yet. As a result, some telcos have connected to Telenor's system for location information, others have no such service at all.

The two major mobile providers in Norway, Telenor and Netcom, have developed two different systems for location information from mobile networks. As a result, the PSAPs must have two different systems to be able to receive location information.

ETSI is working on European standardisation, and a working group called OCG EMTEL is working on user demands for communication to, from and between emergency services. When this group has completed its work, the technical bodies in ETSI will hopefully develop a European standard that will make this a lot easier and less expensive than it is today.

Medland: One major challenge is the number and diversity of organisations that need to be involved. Telcos, of which there are many in the UK, can be encouraged to act by the European Commission and each country's telecommunication regulator. It is not so straightforward with the emergency services, many of which are partly funded and organised at a local government level.

New technical challenges concern knowing where VoIP emergency calls originate.

How much technical and financial effort is required from the telcos to implement the Commission Recommendation on the location-enhanced 112?

Viddal-Ervik: This issue must be divided in two categories: fixed network and mobile network.

For the fixed network the new e-kom law states that telcos must provide location information to the PSAP free of charge. This means that we are not allowed to charge the PSAP for the development of our databases and location information systems.

For the mobile network this is a commercial service.

Medland: This has been mostly completed in the UK. An interface for the transfer of location information was agreed and implemented and the necessary funds provided. The funding is complex – as well as initial set-up costs there are of course ongoing support costs, too. The telcos find the funds for their part of the developments needed – no government funding is provided to them. There is also a dependency on the way emergency services are organised in each country.

As an example, it cost just over 1 million British Pound to provide the new interface to transfer information from four mobile networks to the first stage PSAP in the UK.

What are the main issues concerning privacy?

Viddal-Ervik: The Norwegian law states that calls made to the emergency services override all privacy. This means that if a caller, for example, has caller ID restrictions or an unlisted number, this will be overridden when calls to the emergency services are made.

By when will the Europe-wide, location-enhanced 112 be a reality?

Viddal-Ervik: I cannot answer this question, but I hope soon.

Medland: The EC is due to survey the situation at the end of 2004.

The interview was conducted by Milon Gupta.

The role of OSS in protecting the network

Anastasius Gavras
Eurescom
gavras@eurescom.de

The communication network infrastructure is one of the fundamental elements of today's critical infrastructures. Many other infrastructures, which are essential for a functioning economy and society, such as energy, water, and transportations, depend on a reliable and integer communications infrastructure. It is, thus, worthwhile considering how today's networks achieve the required levels of reliability and integrity. In this context, the operation support system (OSS) is the critical part of the network itself, because it oversees the proper operation of the network.

The managed network

Typically, a network consisting of transmission links and exchange nodes (switches and routers) needs to be managed for a variety of reasons. Networks have grown over the years to become one of the most complex artefacts humankind has invented. In telecommunications, the TMN standards series of ITU-T are the main standards in the management area. The Telecommunication Management Network (TMN) is conceptually a separate network which interfaces a telecommunications network at several different points. The management functions are satisfying requirements that are organised in functional areas, according to the FCAPS principle (Fault, Configuration, Accounting, Performance, Security). The transmission links and exchange nodes are connected via a data communication network to one or more operations systems. The operations systems perform most of the management functions either automatically or via human intervention.

The most important feature of TMN in view of the robustness and reliability of the whole network is the conceptual separation between the network which is managed and the network which transfers the management information. Another important element of the TMN architecture is that it defines a structure for the multiple levels of management responsibility that exist in real networks, known as the Logical Layered Architecture. This has the advantage that understanding and distinguishing the various management responsibilities becomes easier.

Separating the management network from the telecommunications network prevents potential problems with fault management. Even in the case of a failure in the telecommunications network, management will still be able to access the failing components. The down-side of this concept is that additional equipment and transmission systems are required for the management network, meaning increased cost. Nevertheless, the cost is accepted in favour of "five nines" availability, meaning 99,999 % availability of the telecommunications network.

Being a separate network with well-controlled interconnection points, it is also easier to introduce appropriate security measures to protect the management network.

New requirements for NGN?

The vision of next generation networks (NGN) poses significant challenges to an appropriate architecture for operation, administration and maintenance of future networks and services. Along with the pressure arising from deregulation, competition and rapid technology change, the increasing awareness of the importance of the network as part of the critical infrastructure of society poses additional requirements that are being formulated currently. From a perspective of reliability and trustworthiness these requirements inevitably fall in the functional areas of Fault and Security (according to FCAPS).

In many countries the inter-governmental and emergency communications rely to a degree of up to 90 % on public networks. This is the reason why in many countries work is under way to formulate the standards that contribute and support national security and emergency preparedness communications. The issue is also being addressed at the ITU-T in order to foster international co-operation in this area.

New OSS interconnection standards take into account the need for interchange of critical network and service management information between different service providers and the customers. Initiatives have been established to facilitate the interchange of information on service and network disruptions, such as the US National Coordinating Center for Telecommunications.

Conclusion

The network OSS has long been recognised as a critical success factor for supporting existing and emerging business challenges. But the importance of the OSS to support the critical infrastructure of the information society has indeed been identified and is being addressed. The cooperation at the international level has also been recognised and the relevant standardisation bodies, such as the ITU-T and the TeleManagement Forum, are working to establish the necessary standards. It is now up to the commitment of the involved stakeholders, whether nations or organisations, to support this effort as well, since it is not only a technological issue but also includes the learning component for humans involved in the network operations chain.

Milliseconds are vital

Interview with John Cox, CEO of the TETRA MoU Association

The TETRA MoU Association supports and promotes the TETRA standard on radio communication systems for public safety and security. *Eurescom mess@ge* asked the CEO of the TETRA MoU Association, John Cox, about TETRA's contribution to securing critical communication infrastructures for public safety purposes in Europe.

Which communication infrastructures do you consider as the most critical in Europe?

Any communication infrastructure which has an impact on safety of life is critical. However, if a hierarchy of importance has to be established then the most critical will relate to those where safety of many lives is involved as opposed to individuals. These are likely to be those required to deal with major incidents, be they man made or natural disasters. The Public Safety authorities play a major role in such incidents, and it is important that they are able to continue to communicate throughout such events.

There have been many examples of communication failures in such circumstances, which could have been resolved. One of the latest examples is the Spanish rail incident in March 2004, where the public GSM networks were not able to handle the load of calls following the terrorist attack whilst the incident was successfully managed on the TETRA network. It could be concluded from such examples that it would be unwise to rely on public systems such as GSM for backup in times of difficulties due to the overwhelming demands for public communications required.

What are the mechanisms for securing critical communication infrastructures?

There are two key mechanisms to consider: physical security of the network elements and security of the information, which is being passed through the system. The chosen technology has little influence on the physical security of the network elements, switching centres, control rooms, and transmission. Technology choice has some influence at radio sites in the amount and size of equipment required. In the case of TETRA, for example, one single base station unit can provide four separate channels of communication thus saving on space. Transmitted data can be protected by varying levels of encryption although digital radio is inherently more secure than analogue. The different levels of encryption range from full end to end to over the air only using air interface encryption.

How can TETRA help to secure critical communication infrastructures?

TETRA would be installed as a "private" system for use only by those involved in the incident. Control of the network, its physical and transmission security would be in the hands of the users, and the flexibility inherent in the technology would allow the network to be optimised to suit the particular incident, for example grouping users from different disciplines dynamically. Additionally, TETRA is designed with a "graceful" fallback. This means that if transmission is lost between control and the base station site, then the base station site can continue to offer service to terminals within its transmission range unlike public radio systems such as hierarchical cellular systems. If at the next stage the TETRA site is lost, then terminals fall back into what is known as Direct Mode meaning that radios within range can continue to communicate with each other.

Which features of the TETRA system or of other telecommunication systems are the most important for critical communication infrastructures?

Key features are to continue to provide communications throughout an incident. In TETRA this is covered by the fallback communications services mentioned above and the fact that all users are under management control, unlike public networks where systems can become overloaded with uncontrolled public calls.

Also a variety of backbone transmissions networks can be used with multiple routing in conventional network architectures, including IP which not only offers increasing variety of control elements but also a potential reduction in network costs due to high component availability.

Given the increased functionalities of GSM and third generation mobile systems, why are special systems like TETRA necessary?

TETRA is specifically designed for emergency situations and other public safety requirements. Mission-critical features include speed of call setup and group communication. Setting up a call from a TETRA phone takes between 300 and 500 milliseconds, compared to three or more seconds in a public mobile network. Think of a fire alarm, and you will understand how critical setup time is. Milliseconds are vital.

see page 12 ▶▶▶

TETRA and TETRAPOL

In Europe, two major radio systems are used for purposes of public safety and security: TETRA and TETRAPOL.

In addition, it has been explored whether GSM enhanced with ASCI (Advanced Speech Call Items) features could also fulfil requirements for public safety and security.

There have been heated discussions, which system is better, meaning more reliable and more economic. It very much depends on the detailed requirements and personal opinion. Concerning roll-out, this is the situation:

TETRA states that it has currently 505 contracts in 65 countries worldwide. TETRAPOL states that it has more than 70 networks in 31 countries around the globe in operation or being deployed.

TETRA, which stands for TErrestrial Trunked RAdio, is an open digital trunked radio standard defined and supported by ETSI, the European Telecommunications Standardisation Institute.

TETRAPOL has been accepted as a "de facto" standard by the ITU, the CEPT (European Conference of Postal and Telecommunications Administrations), and the European Commission.

References

TETRA MoU website:
www.tetramou.com
TETRAPOL website:
www.tetrapol.com

Another important feature of systems used for public safety purposes are group calls, for example to provide information to all members of a fire brigade at the same time. With TETRA the structure and users in any group can be changed dynamically during the incident with virtually limitless group sizes. This wouldn't be possible to such an extent with currently available GSM or other hierarchical mobile systems, which are designed for individual communication.

To what extent is the TETRA system interoperable with other communications systems?

We have to distinguish between interoperability and interworking. Interoperability in the sense that a terminal could operate across various systems, e.g. TETRA, TETRAPOL, and GSM, is not likely to appear on the market. Interworking between different systems, however, is possible. A TETRA network can be connected to a TETRAPOL or GSM network via a gateway at a switching centre or control room. In this scenario, the special functions of the different systems would be very limited. Another practical problem is that cross-border communication, for example between German and French fire brigades, wouldn't work, because as soon as you cross the border you cannot connect to your own national system with your terminal, because there is no radio coverage.

Real interoperability between national systems is only possible, if all use the same standard. In a recent pilot project in the Aachen region across Germany, Belgium, and the Netherlands, fully interoperable cross-border TETRA services were established.

The ability to have full interoperability between terminals from different networks would require a duplication of coverage. It is sometimes said that duplication is a fail- safe scenario, but it is an expensive one both in terms of cost and environment.

The interview was conducted by Milon Gupta.

Wireless World Research Forum (WWRF)

Shaping the wireless world of tomorrow

Harald Johansen
Eurescom
johansen@eurescom.de

The introduction of GSM in Europe some 15 years ago triggered the growth of a market that can only be compared to the introduction of automatic telephony in the fifties. GSM – now called Second Generation (2G) – has in many regions of the world now replaced fixed line operations.

The world is becoming mobile

Triggered by the success of 2G and the increasing requirement in the market for new mobile and wireless services, third generation (3G) mobile radio systems are currently being deployed in different regions of the world. Considering the lead time for developing enabling technologies, systems beyond the third generation (B3G) are already under discussion in international bodies and fora such as ITU and WRC (World Radio Conference) and they are subject to huge research initiatives in all major trade regions of the world. Based on the experience of the third generation, future systems will be developed mainly from the user perspective with respect to potential services and applications including traffic demands. Systems for a future mobile and wireless world will cover different communications relations as illustrated in figure 1.

Global solutions need a global forum

Mobile and wireless communication has now become a global market, and the development of future systems can only be successful if seen in a global context. By the turn of the century, major public programmes were launched in all trade regions with the aim of boosting research and technology development for future generations of mobile and wireless systems. In 2001, major telecom manufacturers, operators and academia created the Wireless World Research Forum (WWRF) in order to develop common opinions on the wireless world, enable powerful R&D collaborations, and push the wireless frontiers to serve the customers.

A key driver for the WWRF vision is the introduction of I-centric services, adjustable to a vast range of user profiles and

Network operators within the WWRF

- Finnet Group
- Vodafone
- Telefónica
- France Télécom
- Telenor
- BT
- NTT DoCoMo
- Elisa
- Deutsche Telekom
- Portugal Telecom
- TeliaSonera
- Bell Mobility
- Telecom Italia
- Eurescom

Figure 1: Communications in a future mobile and wireless world

needs along with seamless connectivity anywhere and anytime. In addition, such services should be affordable and less expensive than any alternative or traditional solutions. Flexibility, adaptability, reusability, innovative user interfaces, and attractive business models will be the key to the success of the systems beyond the third generation (B3G). To seize the initiative one of the first actions by the newly created forum was to produce a Book of Visions, which outlines this vision of the future and considers the environmental, contextual, and technical aspects.

In Europe, the forum played the initiator role in establishing the Wireless World Initiative (WWI), an umbrella organisation for boosting projects addressing the B3G area within the Sixth Framework Programme of the European Union. Four large Integrated Projects (IPs) have now been launched within the framework of WWI, all addressing key topics for the evolution of next generation mobile and wireless systems:

- MobiLife has a strong user-centric approach and targets issues related to different end-user devices, available communication networks, interaction modes, applications and services. The IP is co-ordinated by Nokia.
- Ambient Networks will enable scalable and affordable wireless networking while providing rich and easy to use communication services for all users. Co-ordinator: Ericsson.
- End-2-end Reconfigurability aims at bringing the full benefits of the valuable diversity within the Radio Eco-Space, composed of a wide range of systems such as mobile, WLAN and broadcast. Co-ordinator: Motorola.
- WINNER deals with new radio technologies and spectrum requirements for future systems. The project is co-ordinated by Siemens.

More than 100 companies, research bodies, and academic institutions are currently working in these projects with more than 3,500 person-months of effort spent per year. Eurescom is providing management support services to MobiLife and WINNER. The WWRF has now turned its attention to the really global issue of bringing opinions and results from similar initiatives in Asia and the Americas together.

Membership

Membership in WWRF is open to all companies, research bodies and academia supporting the promotion and further development of mobile and wireless communications with matching applications and content.

Since its foundation in 2001 WWRF has gained substantial momentum, and the forum has currently more than 150 members, 14 of them are operator organisations.

Organisation

The day-to-day operation of the forum is taken care of by the chairperson, the secretary and the treasurer, assisted by vice-chairs from the Americas, Asia, and Europe/MiddleEast/Africa. Eurescom is providing secretarial and technical support. The current WWRF executives are:

- Chairperson:
  Mikko A. Uusitalo, Nokia, Finland
- Vice Chairperson Americas:
  Miguel Pellon, Motorola, US

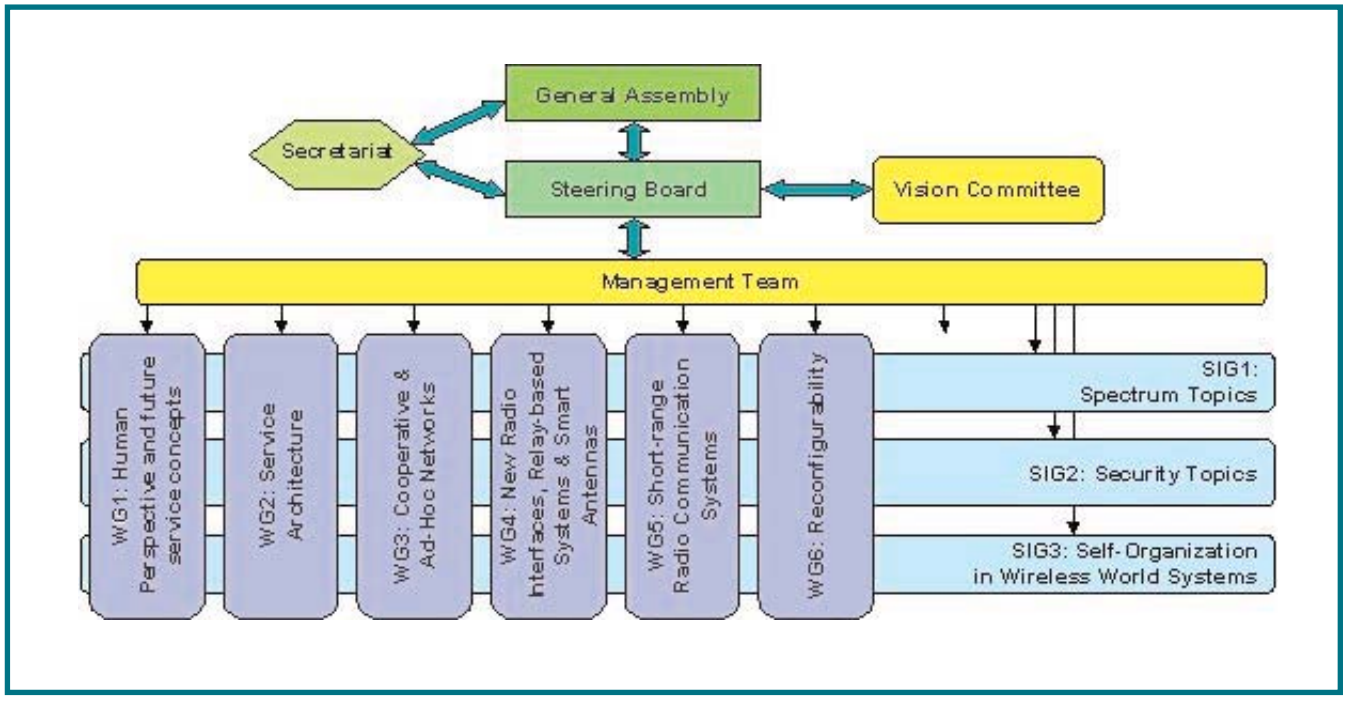


Figure 2: Organisational structure of the WWRF

- Vice Chairperson Asia:
  Young Kyun Kim, Samsung, Korea
- Vice Chairperson Europe:
  Brigitte Cardinael, France Télécom, France
- Treasurer:
  Fiona Williams, Ericsson, Germany

The work itself is organised in six work groups and three special interest groups. A vision committee is drawing up the longer-term visions of the WWRF and producing updates of the Book of Visions on a regular basis. The next edition of the Book of Visions will be available towards the end of 2004.

WWRF is working through meetings

The WWRF is working through regular meetings; three of them per year, one in each of the major trade regions. The meetings offer unique opportunities for both industry and academia to discuss and harmonise their views on all aspects of the future mobile and wireless world. Common positions are formulated in White Papers of which more than 30 are currently progressed. The White Papers serve as an important input to the new edition of the Book of Vision. Whereas the WWRF meetings are open to everybody, the White Papers are only available to members.

The last WWRF meeting took place in Oslo, Norway, in June 2004 and was sponsored by Eurescom and Telenor. The meeting attracted 210 participants who discussed more than 60 high-quality presentations in two days of sessions. The next WWRF meeting will be held on 4-5 November 2004 in Toronto, Canada, hosted by Bell Mobility and Nortel.

Further information is available on the WWRF website at
www.wireless-world-research.org

IST and Quality of Life

Fruitful discussions at the first SOCQUIT Seminar

Peter Stollenmayer
Eurescom
stollenmayer@eurescom.de

A rusty EXPO 92 iron building in Seville allegorising the volatileness of all things. This is the home of the Institute for Prospective Technological Studies (IPTS), which was kindly hosting the first interactive seminar of the EU project SOCQUIT (Social Capital, Quality of Life and Information Society Technologies) from 14 to 15 June 2004.

During the seminar, the consortium partners discussed together with the SOCQUIT Special Interest Group members and some invited guests from the European Commission the first results of the project and on which subjects the focus for the upcoming modelling and analysis work shall be put.

Quality of life in the information society is a hot issue

The seminar was a mixture of presentations and feedback sessions and caused very productive discussions. It was confirmed by all attendees that social capital and quality of life in context with information and communication technologies is a hot European policy topic at the moment. Thorough investigations on how they affect each other and how politics should tackle the issue are important. "With SOCQUIT we are addressing the critical policy issues for the emerging information society," said the SOCQUIT co-ordinator Jeroen Heres from the Dutch TNO.

An overwhelming amount of literature and data is available

The literature and data survey showed that there is an overwhelming amount of literature and data available. "If you enter the search words 'Social Capital' and 'ICT' in Google, you get about 70,000 hits," said Richard Ling, who is leading the related work package. A look at existing survey data sets, which could be re-used for modelling and further analysis, reveals that nearly all Europe is sufficiently covered. The responsible expert Frank Thomas found out that "a review of 45 multi-country and 4 single-country surveys showed that there is sufficient information for a

comparative analysis of Nordic, Anglo-Saxon, Germanic, Latin, and East European ICT users with matched data. The main problem is that the data is not aligned and mostly not longitudinal."

The fundamental question: where to focus?

For the following modelling work and the further detailed analysis it is important to focus on the most relevant topics. The responsible work package leader Ben Anderson from Chimera presented several subjects, which are considered to be of top priority. Amongst them are:

- economic migrants
- groups of people with low quality of life
- broadband Internet usage
- informal communication and quality of life

The seminar participants agreed very much that migrants and economically disadvantaged groups should be amongst the top priority items.

Conclusion

The lively and enthusiastic discussions during the whole seminar showed that SOCQUIT is tackling an important policy issue for the future European information society. The SOCQUIT team will use the discussion results to identify the main topics for further analysis and start working on the related models and analyses.

The presentations – synchronised audio and slides – can be viewed at:
www.eurescom.de/socquit/SOCQUIt-Seminars.htm

Anybody who is interested in SOCQUIT and its results can register on the related portal at:
www.eurescom.de/socquit/Portals/socquit_interest_portal.asp

All registered people will be kept informed of developments in the SOCQUIT project, and become member of an e-mail discussion list.

About SOCQUIT

SOCQUIT is a Specific Support Action (SSA) under Framework Programme 6 with a duration of 20 months, running from December 2003 to July 2005. The consortium partners are TNO (co-ordinator), Telenor, University of Essex (Chimera), Eurescom, and FTR. SOCQUIT provides support for policy, research and industry giving indications of the effects of new IST services on social capital and quality of life, and it initiates expert networks and activities forming the basis for a range of future RTD activities in this subject area.

Further information on SOCQUIT is available at
www.eurescom.de/socquit/

NEMOGS

New market opportunities by GALILEO satellite services

Markus Willner
T-Systems
markus.willner@
t-systems.com

Volker Vierroth
T-Systems
volker.vierroth@
t-systems.com

More and more people are living a life on the move. This new paradigm has changed the way people work, communicate, travel, exchange information, and interact with their environment. Time, speed, location, and a good knowledge of location related issues are core elements to support such a live style.

The NEMOGS study gives an overview on the opportunities GALILEO offers for telecommunications companies. The study's main goal was to identify GALILEO characteristics that are key factors for telco opportunities. Based on these characteristics, potentially beneficial applications and service areas and their business opportunities were elaborated.

The study can be seen as a basic prerequisite for the planning, development and marketing of new GNSS (Global Navigation Satellite Systems) enriched services for telcos.

GALILEO is complementing the existing American GPS system, offering in addition new business opportunities and strengthening existing ones. GALILEO and communication networks are two main components of future context aware solutions. By complementing these with other telco core competencies like authentication, billing and accounting, telcos will play an important role in an emerging new field of applications and services.

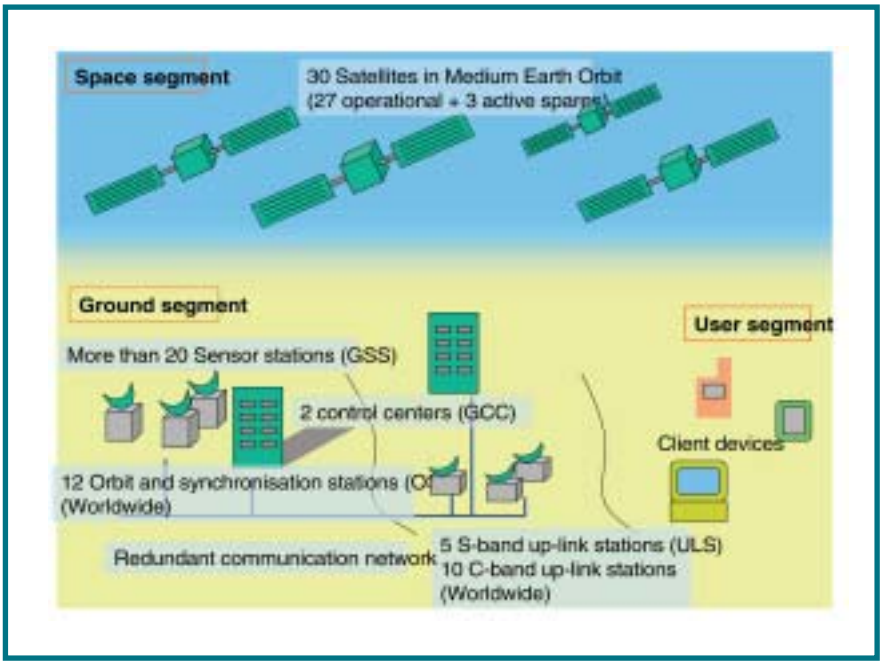


Figure 1: GALILEO system architecture

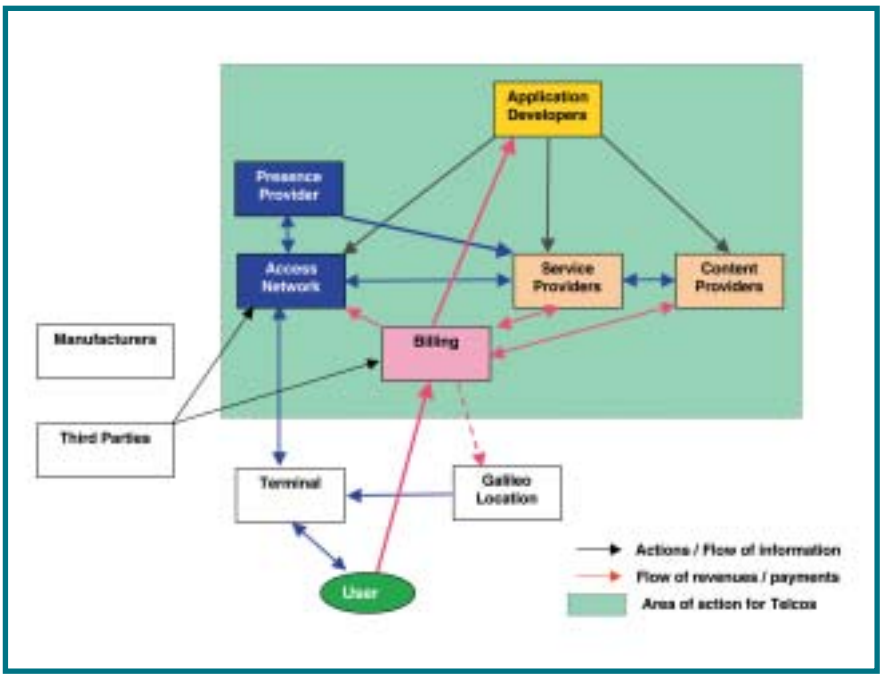


Figure 2: Players, roles and relations in an integrated business case

The European satellite navigation system GALILEO

GALILEO is the name of the upcoming European satellite navigation system. It is currently under development with the first two satellites to be deployed in 2006 and will be fully operational in 2008. The system represents an investment of 3.5 billion euro. It works in conjunction with the US system GPS and adds some important features not available by the latter.

GALILEO is part of the European Union's ongoing endeavour to bring its own technological solutions to the global market place. Currently, the United States have a market share of 100 % for satellite navigation and dependent industries. The entire GPS system is owned and operated by the US Department of Defence. For Europe, the growth of civil mobile services is a promising new market. These new services and markets are highly dependent on location and navigation systems and need full availability anytime, anywhere and from independent providers.

It is expected that GALILEO will open an entirely new market segment to European companies that has been uniquely owned by the US GPS systems before.

The GALILEO architecture consists of three main segments: the Space Segment, Ground Segment, and User Segment (see figure 1).

GALILEO offers five service groups to address different users needs:

- The Open Service results from a combination of open signals, free of user charge, provides position and timing performances competitive with other GNSS systems.
- A Safety of Life Service enhances the open service by adding integrity information.
- The Commercial Service offers higher accuracy and a service guarantee.
- The Public Regulated Service serves the needs of police, fire brigade, emergency and other public institutions.
- The Search and Rescue Service globally broadcasts emergency messages and enhances the existing COSPAS-SARSAT search and rescue system.

GALILEO benefits and opportunities

For GPS, a wide range of devices and applications already exists, ranging from navigation handhelds, built-in navigation systems in cars, boats, airplanes, GPS equipped watches for runners, tourist information systems, diverse gaming and business applications like, for example, management of real estates.

GALILEO opens and extends this immense, world-wide market to European commercial companies and end users.

The NEMOGS study identified four main areas on which telcos should focus, as they offer the highest commercial potential:

- Personal mobility services
- Vehicle telematics
- Gaming
- Supporting or enabling services

The first two areas are the most promising amongst the four, with a revenue share expected to be approximately 80 % of the entire services and applications market, according to most analysts. Two areas are not initially seen as valuable for telcos, but surely will gain momentum after few years of GALILEO's successful market presence: gaming and support services. A market share as high as 20 % seems possible, depending on market development activities and attractive joint offers with suitable partners. Areas with possible telco involvement are shown in the green box in Figure 2.

The number and type of revenue streams varies significantly depending on the level of telco involvement. There are clear benefits and synergies visible, if telcos not only offer their traditional core business, connectivity, but also act as service or billing provider.

Telematics applications and services have not had the long awaited breakthrough yet,

but are a good basis to start for enhanced GALILEO / GPS enabled services.

There is already a broadly installed basis of removable and fixed devices for navigation services in today's cars. This clearly indicates a strong demand, linked to a decreasing price level that in conjunction will lead to a growing mass market. These services will be the pacemakers for other services as indicated in the roadmap in Figure 4.

The roadmap shows applications in order of expected chronological appearance together with GALILEO deployment. The graph gives a clear impression of the challenge for telcos and application developers to follow the tight schedule in order to keep up with this evolution.

Conclusion

All analysed business cases clearly show the importance of the telcos' position in this upcoming new market. Even without being too sure about all possible applications, it can be stated that mobile communication, secure access, authentication and billing are the main enablers for GNSS based, value added services and applications.

The NEMOGS study clearly identified business opportunities for telcos in different areas. The time is right to get prepared for a promising upcoming market. As the roadmap suggests, the perfect time to start is now.

The detailed results of the Eurescom study P1442 are available to Eurescom study programme subscribers at:
www.eurescom.de/public/projects/P1400-series/P1442/

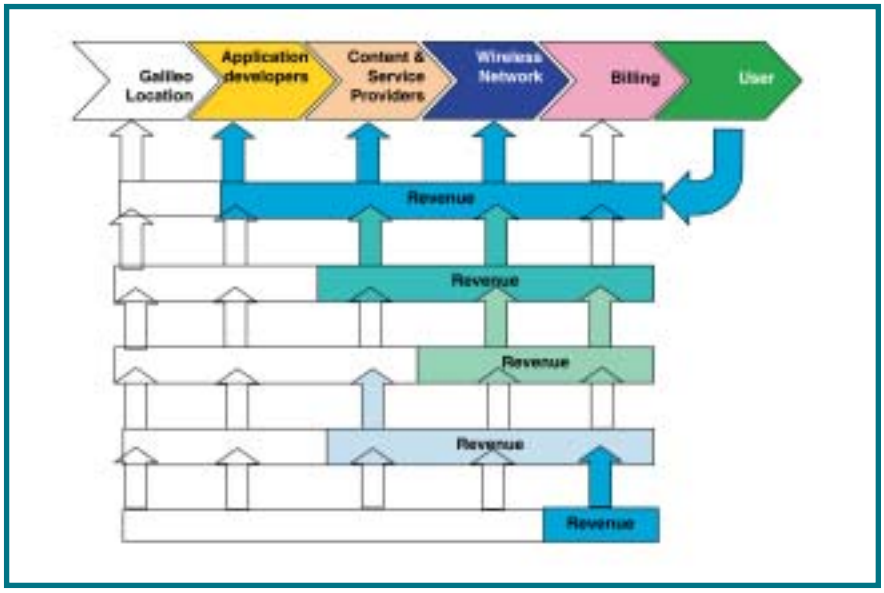


Figure 3: Possible value chains for integrated business case

Figure 4: Roadmap of GALILEO services

GMPLS and MPLS in Enhanced IP Networks

Eurescom project GENIE

Jorge Carapinha
Portugal Telecom Inovaçao
jorgec@ptinovacao.pt

Ferenc Telbisz
MATÁV Hungarian Telecommunications Co. Ltd.
telbisz.ferenc@ln.matav.hu

Nicolai Leymann
T-Systems Nova GmbH
nicolai.leymann@
t-systems.de

Rüdiger Kunze
T-Systems Nova GmbH
ruediger.kunze@
t-systems.com

In the last couple of years multi-protocol label switching (MPLS) has gained a paramount importance for IP service providers, mostly because of its superior capabilities to provide traffic engineering (TE) and virtual private network (VPN) services.

However, MPLS is a technology that is still evolving. Its evolution is driven by the need to manage in a unified framework both the IP and the photonic layers of the networks as well as by the capability of MPLS to become a convergence technology and a common platform for a number of services at the edge of backbone networks. Eurescom project P1305 GENIE has studied the trends in the evolution of MPLS towards GMPLS. This article summarises the main findings of the project and gives statements regarding the development and future role of MPLS.

The evolution of MPLS

MPLS was primarily introduced to ease the routing burden in backbone networks and to allow the building of high-capacity routers by separating routing and forwarding functions. It was soon discov-

ered that MPLS provides an environment in which a range of new services can be offered.

VPNs have been one of the most important MPLS applications. Private networks were previously using ATM or Frame Relay overlay solutions in a "one technology/service, one network" fashion, which meant an inefficient use of the service provider infrastructure as well as high operational expenditures (OPEX). These costs can be decreased with MPLS, for example by emulating and multiplexing Layer 2 (L2) connections, whatever they might be, using point-to-point virtual private wire services (VPWS) and multipoint virtual private LAN services (VPLS).

For this reason, MPLS is changing its role from a pure transport technology to a convergence technology and a common platform for a number of services, which were formerly dispersed through a multitude of technologies (e.g. IP, ATM, Frame Relay, SDH, Ethernet). Figure 1 illustrates how MPLS realises convergence and service aggregation.

With the tests carried out within the GENIE project it was proved that in MPLS networks the connection set-up with different protection mechanisms, load-based routing and routing with topology changes work properly as well as the point-to-point Ethernet services over MPLS. As for the access to the MPLS based VPNs, they can be securely accessed by the end users either via IPSec VPNs or ADSL technology.

Another trend is the development of MPLS towards Generalized MPLS (GMPLS), which is driven by the increasing amount of data traffic and the demand for reducing the cost of network management. It was the objective of the GENIE project to discover challenges that lie ahead of carriers: the rollout of new services, the simplification of service provisioning of existing services as well as the network management and maintenance.

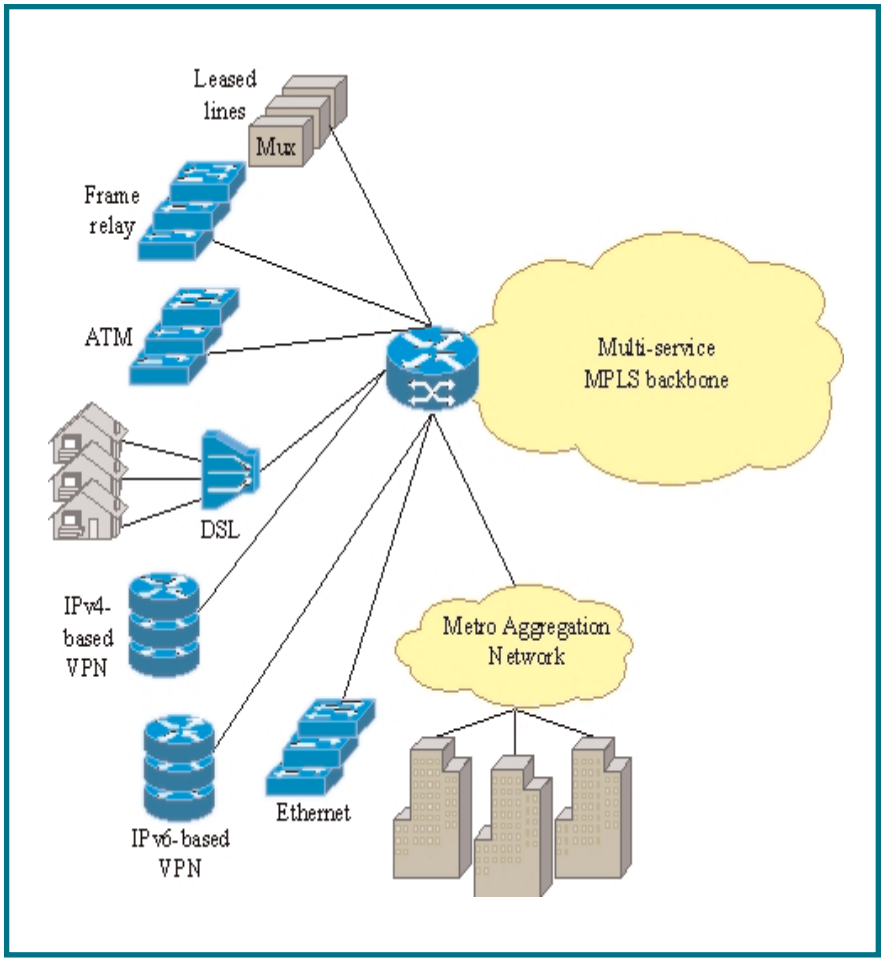


Figure 1: MPLS facilitates convergence and service aggregation.

GMPLS, an extension of MPLS

In the last ten years data traffic increased dramatically. It is widely expected that the predominant traffic carried over data networks will be IP-based, and the slower data streams should be aggregated into streams suitable for optical cross connects (OXCs). The different stages of evolution towards photonic networks are depicted in Figure 2.

The emerging optical networking technologies pose new requirements, which MPLS cannot meet, because it is not designed to this purpose. Unlike IP networks, optical networks are not packet based. Therefore, it became necessary to extend the existing protocols to provide additional support in the time, wavelength, and space domains.

This extension of MPLS is being standardized by the IETF under the umbrella of GMPLS. GMPLS will be an integral part of deploying the next generation of data networks. It provides the necessary bridges between the IP and photonic layers to allow for the interoperability and scalable parallel growth of the IP and photonic worlds.

With GMPLS it will be possible to automate the management and control of network resources and service provisioning. This will enable ISPs to cut down provisioning times dramatically. In the past, several weeks or even months were necessary to provide end-to-end high-speed connections. With the use of GMPLS the provisioning times can be reduced to hours or minutes.

Conclusions and outlook

MPLS has the potential to serve as a common platform for a wide variety of services and finally break the traditional "one-network, one-service" paradigm, something that has been often promised in the past – for example, by ATM and IP – but never actually been delivered.

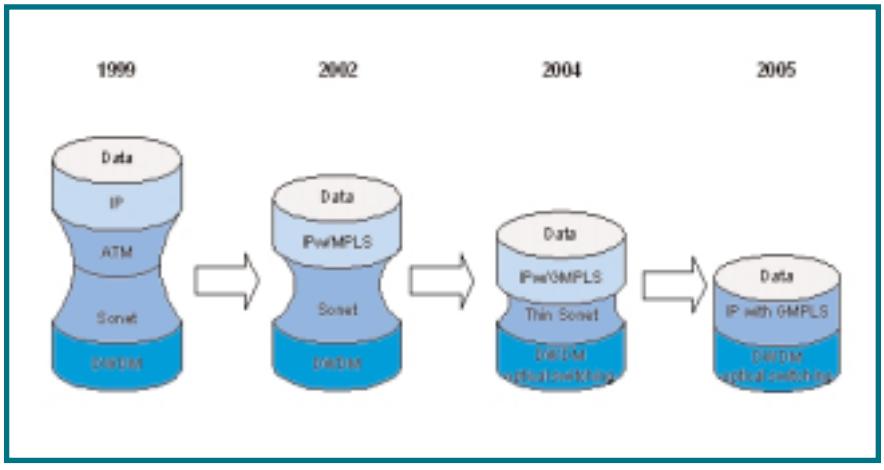


Figure 2: Evolution towards photonic transport networks.

Through the work of the GENIE project it became clear that another very important feature of MPLS is the clear boundary provided by the edge between the backbone and the customer networks. This makes MPLS a future-proof technology, as any upgrade of the services provided to customers can be done without interfering with the transport network. A good example is IPv6: MPLS can facilitate migration by providing IPv6 connectivity between customer domains, with no need to make the core network IPv6-aware, which means without large upgrade investments.

It is the opinion of the authors that MPLS will not remain a technology exclusive to operators, but will become the technology of corporate networks. In particular, large enterprises with several departments spread out to different geographical locations will benefit from the flexibility of the MPLS VPN architecture to manage connectivity and Quality of Service.

GMPLS – the extension of MPLS to the photonic domain – is expected to become an efficient and flexible management tool for the network service providers on all levels of the network after a maturing period and consolidation. GMPLS extends the feature set of MPLS and provides a platform for a dynamic and flexible resource management of packet, time division multiplexed and optical networks. This makes GMPLS an extremely interesting technology for the operators.

Further information on Eurescom project GENIE is available at www.eurescom.de/public/projects/P1300-series/p1305/

ENUM
The bridge between telephony and Internet

Richard Stastny
OEFEG
richard.stastny@oefeg.at

Hans Wallner
Telekom Austria
hans.wallner@
telekom.at

ENUM is a common name for a series of technical protocols and infrastructure arrangements, which fill the gap between the telephone system and the Internet. ENUM is designed to enable global reach of a called party on different electronic communications devices and applications by means of just one identifier – the plain old telephone number.

ENUM is a method to convert traditional telephone numbers into a format that can be used to store and retrieve Internet addressing information, for instance an e-mail address. With ENUM and VoIP (Voice over Internet Protocol) technology, an increasing amount of voice communications can be carried over the Internet instead of over the incumbent telephone network.

VoIP is a method of digitising voice, encapsulating the digitised voice into packets, and transmitting those packets over a packet switched IP network. For the signalling of VoIP calls, several protocols are available; SIP (Session Initiation Protocol) and H.323 are the most popular. This technology has the potential to allow users to save money and to give them more flexibility in their communications by providing additional capabilities such as instant messaging, video, presence and location based services.

How ENUM works

In general, ENUM is a protocol that defines a method to convert a regular telephone number (e.g. for Eurescom +49 6221 989 123) into a format that can be used on the Internet within the Domain Name System (DNS) to look up Internet addressing information such as Uniform Resource Identifiers (URIs). In the regular telephone system, the most significant number appears first, for example the country code +49 for Germany. In Internet domain names, however, the most significant information appears last – for example www.eurescom.de. The country information "de" is last, but will be the first resolved to find the top-level domain (TLD) for Germany.

To arrange the E164 number in an "ENUM format", the protocol reverses the sequence of the digits in an international E.164 telephone number and puts dots between each digit so that each digit becomes a node in the domain name hierarchy. Maintaining perfect coherence between E.164 numbers and their equivalent ENUM names implies that there can be only one official ENUM name space – often called the "Golden Tree". The Internet Architecture Board has proposed the domain name "e164.arpa" for this purpose.

Thus, the ENUM format of Eurescom +49 6221 989 123 would be "3.2.1.9.8.9.1.2.2.6.9.4.e164.arpa"

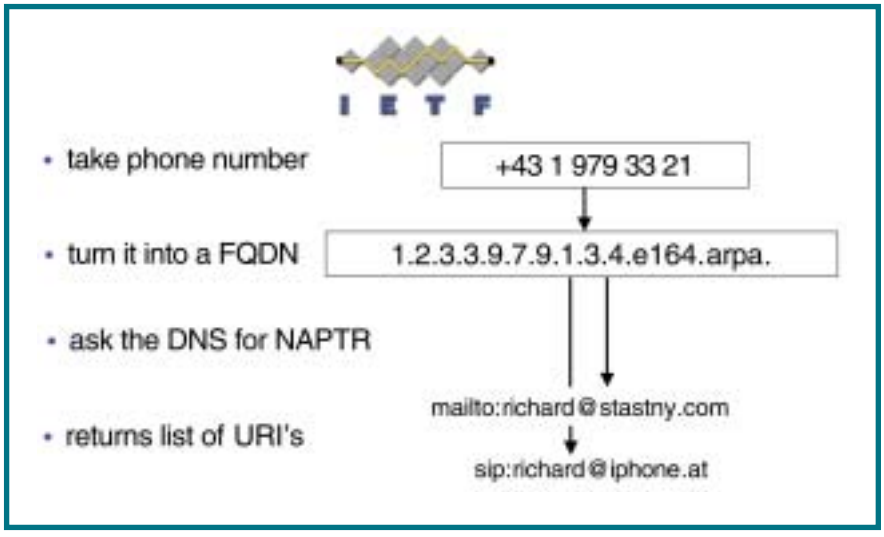


Figure 1: ENUM in a nutshell

The second feature of ENUM is that the Internet addressing Information referred to an ENUM number is stored within the domain name system (DNS), providing routing information to reach the device with the associated ENUM number.

A third feature of the ENUM protocol is that more than one contact information can be stored in the DNS record that is belonging to a specific ENUM number. An ENUM record associated with Eurescom might contain instructions for a VoIP call (e.g. h323:helpdesk@server.eurescom.de or sip:helpdesk@sip.eurescom.de), a facsimile call (e.g. fax: office@fax.eurescom.de), e-mail communications (e.g. mailto:helpdesk@eurescom.de). Additional services can be developed in the future to be included in the ENUM name records.

This facility would allow that the phone number in ENUM will be the single contact number for multiple contact methods for any type of communication (voice, fax, e-mail, mobile, text messaging, location based services, web pages).

What ENUM is not

ENUM does not replace the numeric Internet protocol address (IPv4 or IPv6) that will be used to interact within the IP protocol directly. ENUM has also no role in the conversion of signalling messages and media streams.

ENUM is rather a framework for mapping and processing addresses of different network types. Fundamentally, what ENUM does is to provide another way to determine the desired destination to be used to initiate a communication over the next generation network.

Although ENUM will help facilitate VoIP calls, it is important to understand that VoIP phone calls do not require ENUM, and such calls can be made wholly without ENUM by using their defined Internet addressing scheme (e.g. sip: user@host.com type Address-of-Records).

User ENUM

The User ENUM relies on the technology that is defined in RFC 3761. ENUM assumes a business model, where the ENUM function is provided independently and optionally by ENUM service providers – a form of electronic business card concept or basic buddy list. The phone number becomes a universal key that is globally accessible by all potential correspondents of the user. The data of User ENUM are public. Anyone knowing the universal key, meaning the phone number, can have access to the information, which may have privacy implications. Even if the user subscribes to several applications and services, the user would remain the only party that has the complete control over the set of identifiers.

ENUM is optional not only for the called user, it is also optional for the calling user: the calling user may use ENUM to establish a communication with the called user, but he may also use the conventional method by establishing the call via the PSTN.

This implies that ENUM "domain names" can only be allowed for existing phone numbers and that the domain name holder can only be the assignee of the related E.164 number. Administrative control, meaning proper identification and validation, is necessary to achieve this goal and keep the E.164 numbering plan intact. This is also the reason why the ITU-T and the national regulatory authorities are involved in the administration of the e164.arpa tree.

In summary, User ENUM provides end-users on the Internet (see figure 2) and also end-users on the PSTN (see figure 3) a possibility to find services of other end users on the public Internet.

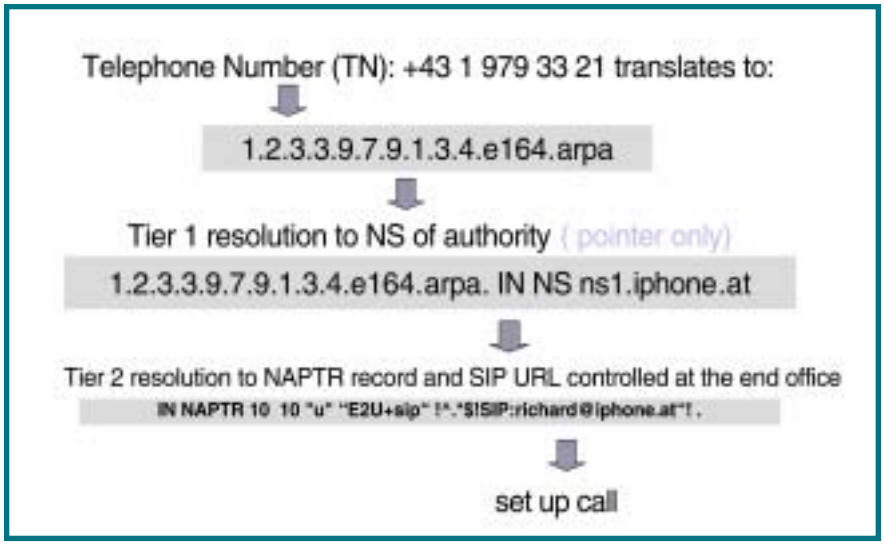


Figure 2: How ENUM works

Infrastructure ENUM

User ENUM is a capability provided for end users and is optional both for the calling and for the called user. If network operators want to use IP-based technology within their networks, they cannot rely on an optional technology used by end users. Instead, they need an independent routing mechanism to find the ingress points to their networks. These network operators are also called IP communications service providers.

If DNS and ENUM technology, as described in RFC3761, is used for this purpose, this is called Infrastructure ENUM. Other terms used are Carrier or Operator ENUM.

The basic principle of Infrastructure ENUM is to provide information only to IP communication service providers, some

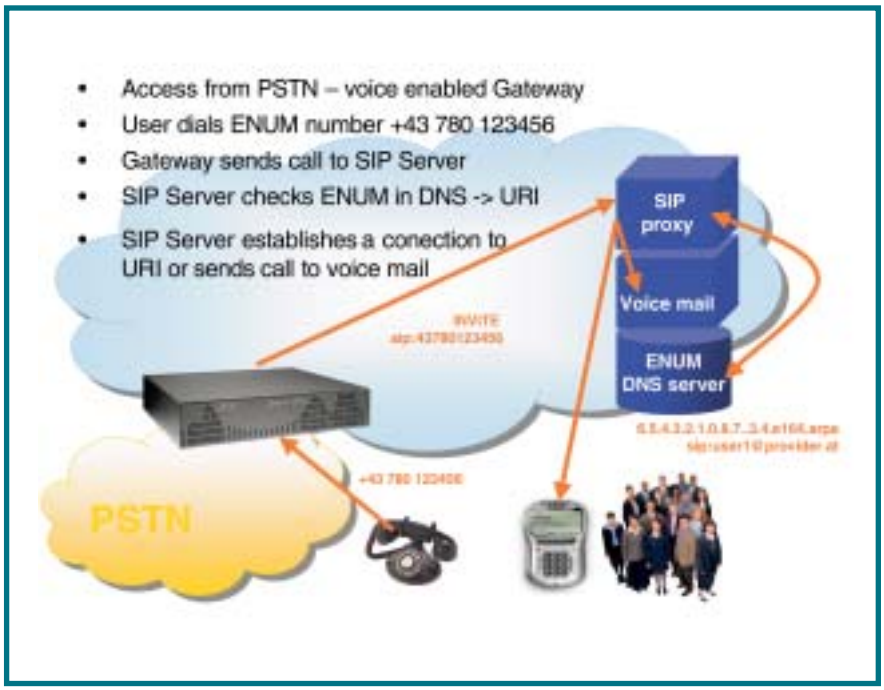


Figure 3: Call from the PSTN to IP

providers may even want to provide this information only to selected peers. The end user has either no access to this information, or he may not be able to use it. This purpose is incompatible with the opt-in principle, because it needs the full population of the information at least for the number range in question. Hence, it must be implemented as an independent system.

If every IP communications service provider is only providing data for numbers hosted by the operator himself, a later merging of trees should not be a problem. If, on the other hand, providers are entering data for numbers they are not hosting themselves (e.g. data for numbers where they provide transit services), then a later merging of trees will cause problems. Therefore, it is not recommended to use Infrastructure ENUM for providing transit information.

Infrastructure ENUM technology may also be used to provide access to national number portability information stored currently in IN databases. The problem with this information is that it has only national significance, for example national routing numbers. This kind of data can therefore not be used directly in supranational Infrastructure ENUM implementations.

Conclusion

User ENUM is an application on the public Internet to provide connectivity directly to end users with E.164 numbers.

Infrastructure ENUM is a routing mechanism to provide IP connectivity between IP-based networks of originating and destination networks of IP communication service providers in addition or as replacement to the PSTN connectivity.

Both systems may be implemented independently.

References

- P. Faltstrom, M. Mealling: RFC 3761 "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", Date: April 2004
- ETSI TISPAN WG: TS 101 172: Minimum requirements for interoperability of ENUM Implementations, V2.0.2 (2004-06)
- ETSI TISPAN WG: Draft TS 101 055 (rev2, 2004-07) Infrastructure ENUM, Work in progress

Further information is available at http://enum.nic.at and http://www.enumf.org

France Télécom takes the chairmanship of the board of Eurescom

In a move that reflects France Télécom's increased commitment to collaborative R&D as a key mechanism for accelerating innovation, Michel Dupire from France Télécom was elected as the chairman of the board of governors of Eurescom.

Mr Dupire has declared that European telcos need to accelerate the pace at which they innovate in order to generate the broad spectrum of services needed on the emerging high-capacity home, wireless, mobile and fixed networks. To this end, France Télécom want to work closely with their peer telco organisations and to give clear signals about how the telcos perceive the future and what types of products are needed.

The telecommunications community is now on the edge of a new era of pervasive converged communications. There is a lot of work to be done jointly to ensure services are portable and interoperable across many different network technologies and terminals. Collaboration at the development stage of these future scenarios is the best strategy for developing an open competitive services market for the benefit of all users and the commercial success of the telcos.

Michel Dupire, Eurescom's new board chairman

Specifically, Mr Dupire sees the integration of home networks with public networks and the cooperation of access networks as a first challenge that the telecommunications community must address. This must allow for the development of a rich set of services which may be accessed any time, anywhere, fully answering the customer's needs, which is the second challenge for the industry.

In his plans for Eurescom, the new chairman promises to refocus the objectives of the organisation to reflect the changing role of the telcos and the critical need for accelerated innovation in the telecommunications sector.

Interconnection of multimedia services

Fireworks project identified gaps in standards

Uwe Herzog
Eurescom
herzog@eurescom.de

A multimedia service originated in one operators network would reach the terminating user in another operator's network only in poor service quality, if current off-the-shelf equipment is used for interconnecting both networks. This is one of the conclusions of the "Fireworks" project on "Interconnection of Multimedia Service Networks". The project identified 13 specific requirements and 29 areas which require further study.

The Fireworks Group was set up in July 2003 by operators in order to profile standards. Eurescom offered to assist the group in their mission, and in March 2004, the Fireworks Group and Eurescom launched a first project on "Interconnection of Multimedia Service Networks".

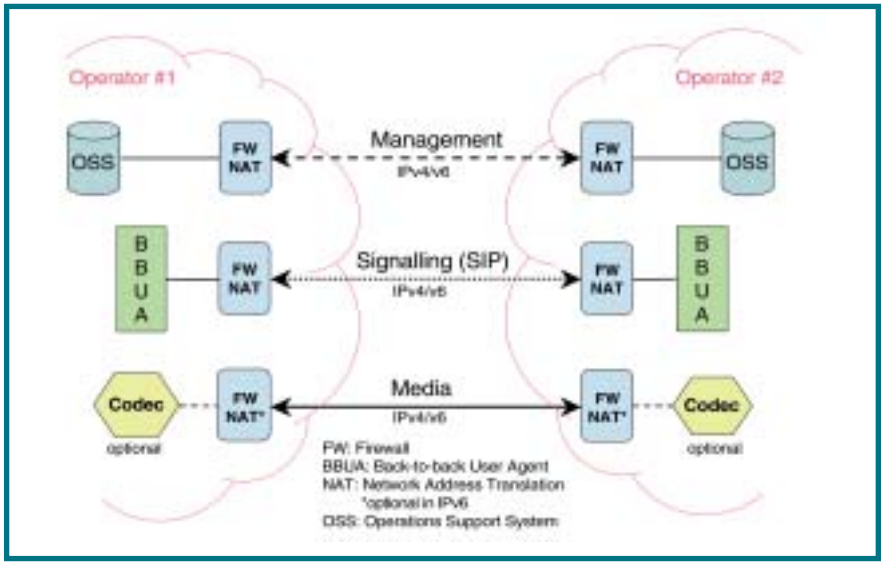
The background of this project was that, from the perspective of operators, the interconnection of IP based networks providing multimedia services has not been given adequate consideration by standardisation yet. Interconnection based on the work done to date is likely to suffer from non-guaranteed QoS, security risks, and inefficient use of network resources. As a result, interworking is only likely to be achieved by bilateral agreements, thus preventing the interoperability of many services.

The below figure sketches the situation at the interconnection point. It shows that there are three types of information flows between interconnected networks:

- Management: service session (e.g. call) unrelated, for network and overall service management
- Signalling: related to the control (setup, modification and release) of specific service sessions and related capabilities.
- Media: user data of the specific service

The final project deliverable describes the technical areas relevant for interconnection and identifies a number of requirements which must be considered, including 29 areas that require further study. "The objective of a follow-up project will not be to specify the missing pieces in the related standards, but to agree on solutions the operators will prefer. The result will be forwarded to the bodies considered most suitable to work on resolving the identified issues," explained Mike Bick of BT.

More information on this project is available at:
www.eurescom.de/public/projects/P1400-series/p1421



Overview of the interconnection point

New Eurescom studies

Another Eurescom study has been kicked off. Some more studies will be started shortly. They will be introduced in the next issue.

WiBAN – WiMAX in Backhaul and Access Networks (P1446)

WiBAN addresses WiMAX (IEEE 802.16a, d and e) and its implications on the business of telcos.

The study team will identify and analyse possible usage scenarios for WiMAX, with respect to new business opportunities, ease of deployment, and possible cost savings. It will focus on questions like: How will WiMAX fit into the telcos' current infrastructure? Will it be complementary to other broadband technologies, or will there be competition? Can WiMAX be used as an enabler for other new technologies like WLAN hotspots?

The possible deployment in urban, suburban and rural areas will be explored, including the use of WIMAX to backhaul different kinds of traffic.

Both the technological and the business aspects of WiMAX will be evaluated from a telco's point of view.

For more information contact:
Christian Hellwig, hellwig@eurescom.de

ENISA
New agency for network and information security

Milon Gupta
Eurescom
gupta@eurescom.de

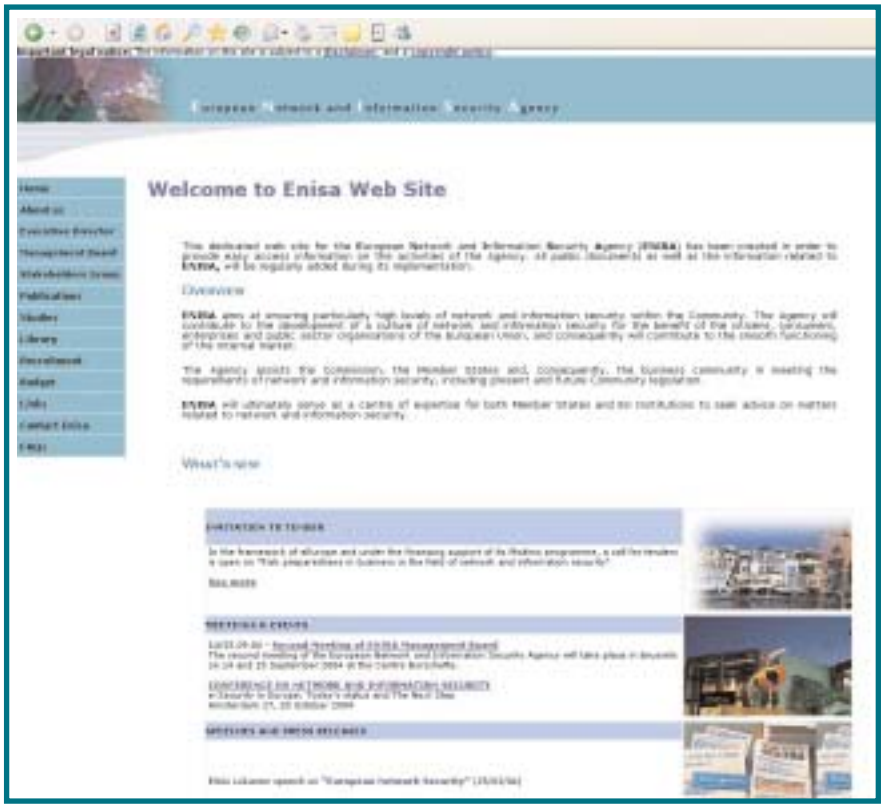
The new European Network and Information Security Agency, ENISA, is expected to become fully operational in autumn with the nomination of its executive director. The Agency was set up in March to enhance the capability of member states and companies in the European Union to prevent, address and respond to network and information security problems. ENISA is located in Heraklion, Greece.

The European Commission regards the work of ENISA as essential to achieve a high level of network and information security within the EU. ENISA will seek to develop a culture of network and information security for the benefit of citizens, consumers, business and public sector organisations in the European Union.

As its in-house expertise grows, ENISA shall help the Commission, the member states and, consequently, the business community to address, respond and especially to prevent network and information security problems. This includes assisting the Commission in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

The creation of ENISA has to be seen against the background of an increasing critical dependency of economy and society on computing and networking, which are becoming ubiquitous utilities like electricity or water supply. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society. This stems from the possibility of problems in key information systems, due to system complexity, accidents, mistakes, and attacks to the physical infrastructures which deliver services critical to the well-being of EU citizens.

The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental to the development of e-commerce. Individuals, public administrations and businesses have reacted by deploying security technologies and security management procedures. Member states have taken several supporting measures, such as information campaigns and research projects, to enhance network and information security throughout society.



ENISA website

The technical complexity of networks and information systems, the variety of products and services that are interconnected, and the huge number of private and public players involve significant risks for the functioning of the European market. In this context, ENISA's activities consist of advisory and coordinating functions, data analysis, as well as raising awareness and cooperation.

Among other things, the agency provides assistance to the Commission and Member States in their dialogue with industry to address security-related problems in hardware and software products.

ENISA will focus on four main tasks:

- Firstly, advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Secondly, collecting and analysing data on security incidents in Europe and emerging risks.
- Thirdly, promoting risk assessment and risk management methods to enhance the capability to deal with information security threats.
- Finally, awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.

ENISA will also follow the development of standards, promote risk assessment activities and interoperable risk management routines and will produce studies on these issues, involving public and private sector organisations.

Further information is available on the ENISA website at
www.enisa.eu.int

The European Security Research Programme

Europe's response to rising security threats

Anastasius Gavras
Eurescom
gavras@eurescom.de

Political, social and technological developments have dramatically changed the security environment where risks and vulnerabilities are more diverse and less visible. New threats have emerged that ignore state borders and target European interests outside and within EU territory. In December 2003 the European Council adopted a common EU security strategy, recognising the need to further develop the capabilities to protect its citizens and contribute to a safer international environment.

The underlying proposition is that Europe must take advantage of its technological strengths to guarantee security. Although technology alone cannot guarantee security, without the support of technology, security does not seem feasible today. New technology trends offer new opportunities. Civil, security and defence applications increasingly draw on the same technological base – creating new synergies between different research sectors. The Group of Personalities (GoP – see box) recommends in its report a European Security Research Programme (ESRP), which should take advantage of the duality of technologies and the growing overlap of security functions to bridge the gap between civil and defence research. In support of a comprehensive security approach, the ESRP should fund research activities targeted at the development of systems and products that could be used, for example, to protect European critical infrastructures against transnational threats.

The GoP report points to structural deficiencies at institutional and political level which hinder Europe in the exploitation of its scientific, technological, and industrial strength. In order to overcome these deficiencies, Europe needs to increase its funding and improve the coherence of its efforts, according to the recommendations of the GoP. This implies:

- effective coordination between national and European research activities,
- systematic analysis of security-related capability needs, from civil security to defence,
- full exploitation of synergies between defence, security, and civil research,
- specific legal conditions and funding instruments for security-related research at the European level, and
- institutional arrangements that are efficient and flexible enough to combine Member-State and Community efforts and to involve other interested partners.

In its report, the GoP lays out the cornerstones of a European Security Research Programme (ESRP) and recommends a minimum annual budget of € 1 billion with the possibility to progressively increase it further, if appropriate. The ESRP is seen as an instrument to foster cross-border cooperation, increase European industrial competitiveness, and to strengthen Europe's research base. The recommendation has a European scope and in itself is a precondition for numerous EC policies in sectors like transport, energy, and telecommunication.

Communications are a key aspect

Although each threat may have its specificities, an effective defence against them will often require the same missions. Border control, for example, is an important mission in the fight against proliferation, organised crime, and terrorism. However, the protection of communication networks as elements of critical infrastructures is also essential in the fight against terrorism and organized crime.

The ESRP has a strong background in defence and border control missions, but recognises the importance of networks for

The Group of Personalities

The primary mission of the Group of Personalities in the field of security research has been to propose principles and priorities of a European security research programme. This programme is aimed to be in line with the EU's policy objectives in the areas of foreign policy, security, and defence and based on the principles of freedom, security, and justice. Co-chaired by European Commissioners Busquin and Liikanen, the Group was composed of eight chairmen and chief executives from the security industry, four serving members of the European Parliament, four heads of major research institutes, two high-level European defence ministry officials, and two high-level political representatives from EU member states – a former prime minister and a former president. Heads of various international organizations and the High Representative for the Common Foreign and Security Policy (CFSP), Javier Solana, also participated in the work.

The group had worked for six months towards developing the cornerstones of a EU security research programme and the contribution this programme could make to address the new security challenges in a changing world. On 15 March 2004, the Group of Personalities (GOP) for Security Research issued a report of entitled "Research for a Secure Europe". This report calls for at least € 1 billion per year to be provided for security-related research within the EU's Framework Research budget, starting in 2007.

Report of the Group of Personalities:
http://europa.eu.int/comm/research/security/pdf/gop_en.pdf

both internal security and crisis-management operations as a key aspect. Security management is inherently distributed across different authorities and operators, with their respective roles, capabilities, and resources. In such a decentralised environment, interoperability of communication and information systems and the links between different networks are crucial. All relevant security services should be able to exchange information rapidly and securely, and this information should be made available via communication means whenever and where ever needed.

Preparatory action

Following the adoption of the EU security strategy, the European Commission launched a preparatory action on the "Enhancement of the European industrial potential in the field of Security Research 2004-2006" for addressing key security challenges facing Europe and its partners. Under the Preparatory Action on Security Research (PASR), 175 proposals were submitted in response to the European Commission's call for proposals, which ran from 31 March to 23 June 2004.

These proposals aim to research, validate and integrate security-oriented technologies and capabilities in five areas:

- Situation awareness
- Protection of networked systems
- Protection against terrorism
- Crisis management
- Interoperability of control and communications systems

The 2004-2006 PASR initiative has allocated € 65 million of EU funding for the three-year projects, of which € 15 million will be released in 2004. Total funding for all of the selected proposals will be approximately € 300 million, including the contributions from project participants. The successful conclusion of the projects should pave the way for a leap in EU funding for security research, according to the recommendation found in the report of the Group of Personalities in the field of Security Research, entitled "Research for a Secure Europe".

European Security Research Programme on the Web
http://europa.eu.int/comm/research/security/index_en.html

new project results

EURESCOM STUDIES

P1347 **Online Console Gaming**
Deliverable 1 · Online Console Gaming – A whole new game? · Eurescom Study Programme confidential

P1349 **TelcoGrid: Business Opportunities for Telecom Operators in the Grid Market**
Deliverable 1 · Business Opportunities for Telecom Operators in the Grid Market · Eurescom Study Programme confidential

P1349 **TelcoGrid: Business Opportunities for Telecom Operators in the Grid Market**
Deliverable 2 · Business Opportunities for Telecom Operators in the Grid Market (presentation) · Eurescom Study Programme confidential

P1350 **MASMO – Multi-Application Smart Card Market Opportunities**
Deliverable 1 · Multi-Application Smart Card Market Opportunities Eurescom Study Programme confidential

P1350 **MASMO – Multi-Application Smart Card Market Opportunities**
Deliverable 2 · Multi-Application Smart Card Market Opportunities (presentation) · Eurescom Study Programme confidential

P1441 **IDA3 - Identity Management enabled AAA Services**
Deliverable 1 · Impact of combined IdM- and AAA services Eurescom Study Programme confidential

P1441 **IDA3 - Identity Management enabled AAA Services**
Deliverable 2 · Strategic recommendations on ID Management Enabling AAA services · Eurescom Study Programme confidential

P1441 **IDA3 - Identity Management enabled AAA Services**
Deliverable 3 · Comprehensive presentation of ID Management enabling AAA services · Eurescom Study Programme confidential

P1442 **NEMOGS - New market opportunities by Galileo satellite services**
Deliverable 2 · Potential applications and services, business aspects Eurescom Study Programme confidential

P1442 **NEMOGS - New market opportunities by Galileo satellite services**
Deliverable 3 · Potential applications and services, business aspects (presentation) · Eurescom Study Programme confidential

EURESCOM PROJECTS

P1302 **PROFIT: Potential pRofit Opportunities in the Future ambient InTelligence world**
Deliverable 5 · Strategic Recommendations for Telcos · Eurescom confidential

P1402 **TIMES – The Inter-operator IM and Mobile IM service**
Technical Information 1 · Overview and trial preparation · For full publication

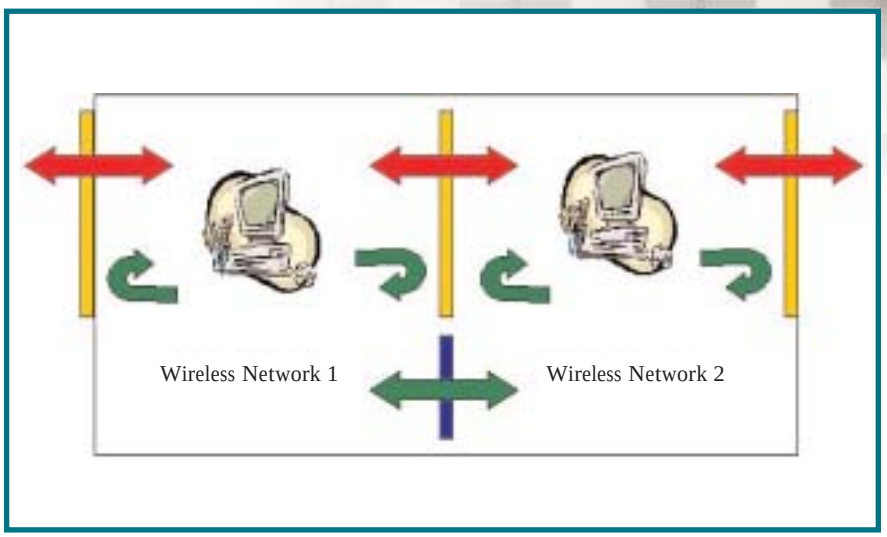
Stealthy wallpaper

Novel interior decoration for wireless security

Milon Gupta
Eurescom
gupta@eurescom.de

What do a stealth bomber and your four walls have in common? At the moment almost nothing, but this may change soon. A spin-off from stealth aircraft radar signature control technology is ready to innovate the interior design of high-tech offices and paranoid-geek homes. British defence company BAE Systems has developed a "stealthy wallpaper" which is designed to block uninvited radio transmissions.

What differentiates the "stealthy wallpaper" from conventional barriers against radio waves – like, for instance, frequency-absorbing foam or metal – is its ability to filter frequencies. This allows you to receive a mobile phone call while your Wireless LAN is blocked.



How it works: Passive wallpaper (gold) permits mobile telephone signals (red) to pass but blocks WLAN transmissions (green). If required, active wallpaper (blue) can be used to allow WLAN transmissions to propagate when turned on and to maintain isola-tion when turned off.

Frequency selective surface

The trick is done by a frequency selective surface (FSS), which is very thin – 50 to 100 microns (millionth of a meter). BAE Systems designed several types of FSS. One is aimed at blocking WLAN transmissions while permitting signals in the UMTS bands to pass through. Other designs permit passbands corresponding to the IEEE802.11b and IEEE802.11a communications standards to be enabled and disabled at the touch of a button. The material can be applied to ordinary structural and partition walls. For application to windowpanes, transparent conductors can be used.

Military spin-off

The basic principles of the frequency selective surface are identical to those of materials used in aircraft radar signature reduction. Where the "stealthy wallpaper" differs is that it is not incorporated into a structural radome and is a thin, flexible material. It does not require the addition of extra dielectric layers to preserve its characteristics at high incidence angles or provide a sharp filter response.

Work on the project began in May 2003 and culminated in a full-scale demonstration in May 2004. The short development time is easily explained: the team working on the "stealthy wallpaper" project has more than 25 man years experience in the field of frequency selective surfaces.

Commercial use

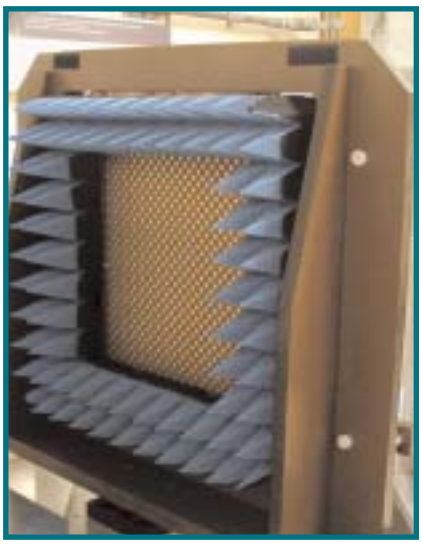
Kevin Mitchell, project manager at BAE Systems Advanced Technology Centre, Filton, envisages two major applications: "Firstly, isolation of WLAN transmissions for enhanced network security. Secondly, control of WLAN signals with the aim of reducing interference and hence allowing more networks to exist in close proximity."

In the initial marketing phase, he expects large corporations who want to improve the security of their wireless networks to be the main customers. "The domestic consumer market may follow, particularly if wireless technology is widely adopted in areas of high-density housing, and interference between networks becomes significant," said Mr Mitchell.

Regarding the cost, BAE Systems claims that their "stealthy wallpaper" is no more expensive than conventional methods of screening, because only conventional PCB materials and manufacturing processing need to be used.

BAE Systems is currently exploring how best to bring the product to the market. This may involve licensing designs, a spin-off company or some form of partner-ship with an existing operator in the civil communications field, according to Mr Mitchell. There is no planned launching date yet, but Mr Mitchell is confident that "given the maturity of the technology, it is possible that a product may be commercially available in a short timescale."

Until this happens, the best remedy to protect your Wireless LAN against nosy neighbours and worrisome wardrivers, who want to eavesdrop on your data communication, will be to get your WEP (Wired Equivalent Privacy) settings rights.



Testing the "stealthy wallpaper" at the BAE Systems Advanced Technology Centre in Bristol. The "stealthy wallpaper" consists of a frequency selective surface, which is 50 to 100 microns thin.

Eurescom FP6 proposal and project services

On behalf of its member companies, major telecoms companies, Eurescom has successfully participated in the EU 6th Framework Programme. Eurescom's unique FP6 services are now also open to suitable non-members.

The scope of our FP6 services covers the whole life cycle of a project, from the preparation of project proposals to the implementation of the project and the exploitation of project results.

The Eurescom FP6 services include:

Project preparation
- Feasibility analysis
- Consortium building
- Consortium agreement
- Consortium support
- Proposal writing
- Proposal evaluation

Project implementation
- Project reporting service
- Standard website
- Communication and FTP tools
- Administrative support
- Project management

Exploitation of results
- Standardisation input
- Technology transfer
- Workshops & conferences
- Public Relations campaigns
- Training

Please contact us at info@eurescom.de, if you are interested to use our services.

EURESCOM CONFERENCE CENTRE

The innovative venue for business events in Heidelberg

The Eurescom Conference Centre (ECC) is one of the most exclusive meeting places in Europe. It consists of a modernised villa and a new building, both with fully equipped conference facilities.

The ECC is located in five minutes driving distance from the famous Heidelberg castle in one of the most beautiful quarters of the city. The nine conference rooms offer ideal opportunities for business events, ranging from small meetings to conferences with more than 100 participants. At the ECC, visitors will find a unique blend of the distinguished atmosphere in the historic Villa Reiner with its beautiful park and the innovative ambience in the modern building.

The experience of Eurescom in organising international conferences guarantees a professional event service, which will also meet special requirements.

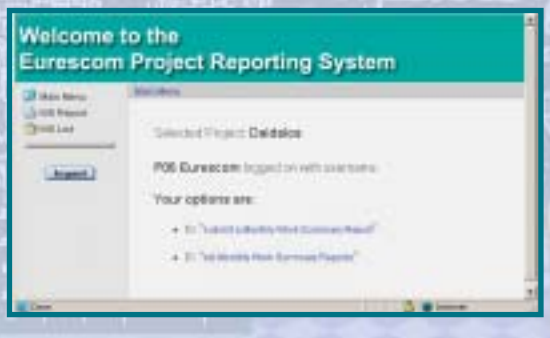
Address:
Eurescom Conference Centre, Schloss-Wolfsbrunnenweg 35,
69118 Heidelberg, Germany

Contact:
Carmen Tomaszewski,
phone: +49 6221 989-250,
e-mail: tomaszewski@eurescom.de

Please ask for our brochure.

Next issue – December 2004:
Usability of end-user devices

EU Project Reporting – Fast and Easy



"Before I had Eurescom Project Reporter, the reporting was cumbersome and it took a long time to get a good overview. Now it is much easier, and I can access the current project data whenever I want. A great tool! However, partners still have to report in time."

Riccardo Pascotto, Deutsche Telekom
Project coordinator of EU Integrated Project DAIDALOS

EU project reporting can be so fast and easy – with Eurescom Project Reporter. Forget about cumbersome, self-made spreadsheet files that have to be uploaded on some server in some directory you always forget. Eurescom Project Reporter offers you an easy-to-use web interface tailored to every partner, which makes entering work and financial data as well as getting a quick overview on the current budget status for EU FP6 Integrated Projects and other EU projects a matter of minutes.

Further information about Eurescom Project Reporter is available at **www.eurescom.de/services**

There you will also find information about our other services for EU/collaborative R&D projects.
Contact us at **projectreporter@eurescom.de**

EURESCOM

European Institute for Research
and Strategic Studies
in Telecommunications GmbH
Schloss-Wolfsbrunnenweg 35
69118 Heidelberg, Germany
Tel.: +49 6221 989-0
Fax: +49 6221 989 209
E-mail: info@eurescom.de
http://www.eurescom.de

Innovation through collaboration

Eurescom is the leading organisation for collaborative R&D in telecommunications. Our mission is to provide efficient management of research projects and programmes for member companies and other clients. We offer more than ten years of experience in managing large-scale distributed R&D using a dynamic network of experts. Companies who wish to collaborate on the key issues facing the telecoms industry are welcome to join the Eurescom community.