EURESCOM mess@ge

The magazine for telecom insiders

NEWS

Celtic-Plus
Smart Connected World

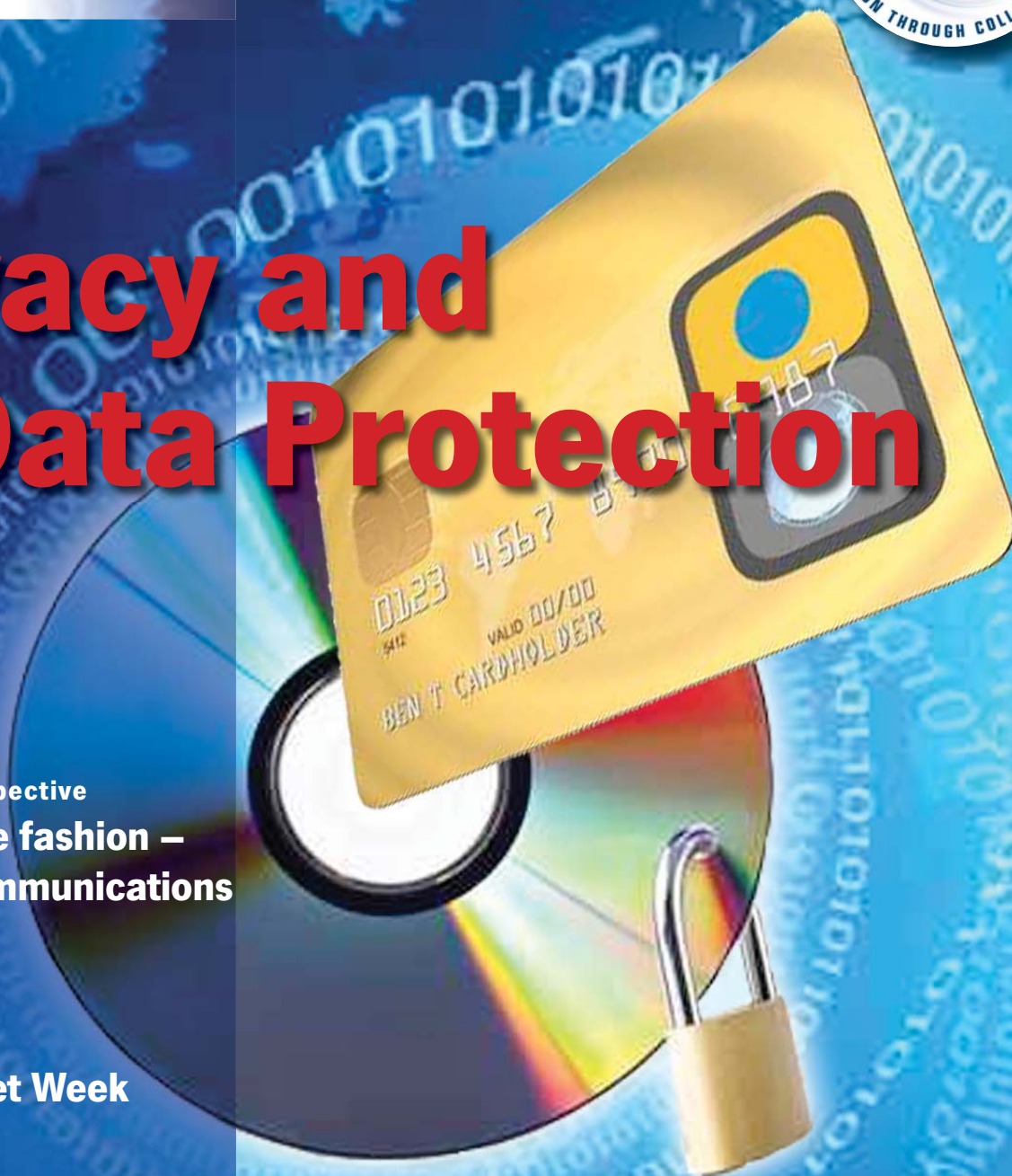**20 YEARS** OF INNOVATION THROUGH COLLABORATION

Privacy and Data Protection

The Kennedy perspective
**Retro is all the fashion —
except for communications
devices**

Events
**Future Internet Week
in Poznan**

A bit beyond
**ICT and the next billion
people**

Celtic-Plus Calls for Proposals in 2012

In 2012, Celtic-Plus will run two proposal calls for fully defined project proposals according to the following schedule:

> 2012 proposal submission deadlines:
> ❯ Spring call: **21 March 2012**
> ❯ Autumn call: **10 October 2012**
> The total budget volume in 2012 is expected to be up to 100 million euro

The following research areas are possible (see also Celtic-Plus Purple Book):

Get Connected
- Infrastructure and connectivity aspects
- Fixed/ Wireless, optics, energy-efficiency
- Network architecture , autonomic networks

While Connected
- End-to-end services and applications, like
  - Digital home, digital enterprises
  - Digital City (incl. digital school, digital transport)
  - E-Health
  - Security, privacy, identity

Future Internet relations
- Complement Future Internet (FI-PPP) program by
  - Making the Internet a high-quality service platform
  - Introduce the 'Celtic-Plus Use-Case Factory'
    - Extend the program by additional use-cases not covered in the FI-PPP program
    - Contribute to future internet capacity building and test cases/ platforms

Green-Internet relations
- Consider environmental issues in ICT
- Encourage better energy efficiency
- Consider Smart Grid, Water management & ICT
- Develop multi-disciplinary approach

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

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

Further information
For further information, please contact Heinz Brüggemann, director of the Celtic Office, at brueggemann@celticplus.eu

http://www.celticplus.eu

Celtic-Plus will run its 7th annual conference, entitled "Celtic-Plus Event 2012 – Realising the Smart Connected World", in Stockholm, Sweden, from **22 to 23 February 2012**.

Interested researchers and high-level managers from industry and public authorities are invited to attend. The number of participants is limited to 200 people! For registration please follow the link: **http://www.celticplus.eu/Events/Event2012/registration.asp.**

Highlights of the programme and the new Celtic-Plus research areas are in particular:

- New, infrastructural telecommunication challenges for secure, high-speed and ubiquitous networks
- New service challenges, like digital/ smart home, digital/ smart cities, e-Health, etc.
- Future Internet topics in complement to the EU FI-PPP initiative (e.g. to build up a Celtic-Plus ''Use Case Factory'', as well as new inter-disciplinary challenges related e.g. to smart energy, green ICT, and CleanTech ''grand challenges'')

The event will be complemented with an exhibition of project results from a selected number of important Celtic projects.
Further information and registration access are available on the Celtic-Plus Event web site at http://www.celticplus.eu/Events/Event2012/default.asp

Heinz Brüggemann · Director Celtic Office
Wieblinger Weg 19/4 · 69123 Heidelberg/ Germany
Tel: +496221989210 · Mobile: +491713309452
 http://www.celticplus.eu

Dear readers,

The importance of privacy and data protection has been increasing in parallel to information and communication technologies becoming ever more pervasive. Whether it is online banking, air travel, or social networking – ICT is permeating all aspects of our social life. This has been driven by a rapid development pace of technologies which were not known, when the still valid EU data protection rules were introduced in 1995. These rules are currently being updated by the EC in order to better protect the citizens' privacy in a dynamically changing digital world, while at the same time enabling the ICT industry to provide innovative services without putting them under stifling compliance pressure.

Recent events worldwide have shown, how important privacy and data protection have become due to the pervasiveness of digital services. The hacking of Sony customer data in April 2011 has shown, how vulnerable personal data can be nowadays. Apart from data-collecting global companies, like Facebook and Google, or criminals going after customer accounts and credit card data, there is also the issue of state intrusion into citizens' privacy. The recent debate in Germany about the limits for using Trojan software for surveying the PCs of suspects has highlighted the issue.

Against this background, the editorial team of Eurescom mess@ge decided it is about time to dedicate a cover theme to privacy and data protection. In this issue, we will not only highlight the challenges, but also the opportunities involved in managing and protecting private data.

In the first article, you will get an overview on some of the issues and developments regarding privacy and data protection in Europe. The ensuing article by Ricardo Azevedo Pereira from Portugal Telecom Inovação highlights technological trends and issues in identity management and discusses opportunities for telecoms network operators.

In an exclusive interview, European Data Protection Supervisor Peter Hustinx shares his views on important data privacy questions in Europe and the requirements for the EU's new data protection framework.

Aljosa Pasic from Atos, who is also board member of the European Organisation for Security, presents an industry perspective on privacy issues, with a particular focus on the concept of Privacy by Design.

Finally, Dr. Matthias Baumgart from Deutsche Telekom Innovation Laboratories provides a report on the results of a Eurescom study on how to secure devices based on the Android operating system.

This selection of articles does not cover all aspects of privacy and data security, but it provides insights on some major challenges, opportunities and solutions.

This issue also includes reports on three important European research events, the NEM Summit in Torino, the Net!Works General Assembly in Brussels, and the Future Internet Week in Poznan. See also the articles in our sections "The Kennedy Perspective", "News in brief", and "A bit beyond". I hope you enjoy reading them.

My editorial colleagues and myself would appreciate your comments and suggestions for future issues.

Milon Gupta
Editor-in-chief

Events calendar

5 – 6 December 2011
Innovation Convention 2011
Brussels, Belgium
http://ec.europa.eu/research/innovation-union/ic2011/
index_en.cfm

13 December 2011
EU research and innovation: What role for regions and cities after 2013?
Brussels, Belgium
http://www.cor.europa.eu/pages/EventTemplate.aspx

22 – 23 February 2012
Celtic-Plus Event 2012
Stockholm, Sweden
www.celticplus.eu/Events/Event2012/default.asp

27 February – 1 March 2012
Mobile World Congress
Barcelona, Spain
http://www.mobileworldcongress.com

6 – 10 March 2012
CeBIT
Hanover, Germany
http://www.cebit.de/home

8 – 9 March 2012
Third Augmented Human International Conference (AH 2012)
Megève, France
http://www.augmented-human.com

7 – 9 May 2012
eHealth Week 2012
Copenhagen, Denmark
http://worldofhealthit.org/2012

10 – 11 May 2012
Future Internet Assembly
Aalborg, Denmark
http://www.future-internet.eu/news/view/article/future-internet-
assembly-aalborg.html

28 May – 1 June 2012
The IFA 11th Global Conference on Ageing
Prague, Czech Republic
http://www.ifa2012.com

4 – 6 July 2012
Future Network and MobileSummit
Berlin, Germany
http://www.futurenetworksummit.eu/2012

Sn@pshot

Handyman robot in space

Robonaut 2 is a dexterous humanoid robot built and designed at NASA Johnson Space Center in Houston, Texas. The robot's purpose is to help humans work and explore in space. On 13 October 2011, Robonaut 2 successfully moved for the first time in space.
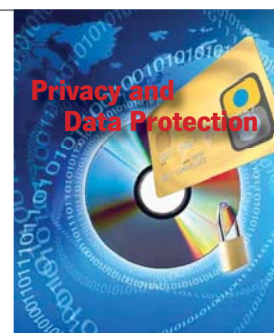
Further information is available at
http://robonaut.jsc.nasa.gov

Contents

NEWS

Retro is all the fashion –
except for communications devices

David Kennedy
Director of Eurescom
kennedy@eurescom.eu

My hobby is old cars from the 60s and 70s. This led me to thinking about what the equivalent in telecommunications would be. Will it be first generation GSM phones in 20 years time? Will we happily use them, because they remind us of a time when technology was relatively simple and voice and SMS were the only available apps?

The interesting question is, if we can revive previous generations of technology as retro fashion items or just for the enjoyment of using more basic devices.

Home phones

Already we have seen the move from the phone being a single device in a preserved place in a home to being a portable device which enabled us to even receive calls in the bathroom. While in many networks the exchanges still understand decadic signalling, it is slowly being phased out. This means that an original dial telephone will soon be obsolete. My daughters are 13 and 15, and they have never used a dial phone. They will never know the fun of using a big black Bakelite phone and waiting for the dial to return from dialling "0" in its unhurried way.

Now people can make phone calls from wireless DECT phones, PCs, iPads, and all sorts of clever devices, without ever thinking about the huge machine that must exist to support their global connectivity. I think we have lost something here. Communication used to be a special occasion. Now it is an expected commodity.

Backward compatibility only goes so far

Clearly we cannot resort to analogue mobile phones, as the networks for these are now gone. We have to stay with mobile phone technology from at least after the first GSM call was made by Radiolinja in Finland in 1991, 20 years ago - by the way, the same year Eurescom was founded.

In 2006 the number of GSM connections exceeded two billion customers, which can only be described as a phenomenal growth. Maybe this speed of growth is one of the factors that prevents us from desiring a return to more retro feeling services. The old versions were not around long enough for them to become icons – except maybe the famous "brick" mobile phone. Today, we are more interested in having the latest most complicated gadget laden smart-ass phone, than having a perfectly functioning "antique". My children have already disposed of several phones, and they are not yet old enough to vote.

No first generation Internet nostalgia

If we consider the Internet, our most important satisfaction parameter is the speed of response. We don't really care if it is the computer, the connection or the server we are talking to as long as it reacts quickly. In this case we are unlikely to accept any retro technology if it means that our user experience is diminished.

Similarly it is difficult to get nostalgic about something that has been part of our life for such a short time. Is Web 1.0 actually over or is it still running? I can't see any chance for any retro equipment to survive, except in technology museums, as we will never accept using old dial up modem speeds of 75/300 baud for "fun" when we are used to Mb/s.

The interesting thing about speed is that it is perhaps why we can enjoy old cars. In 1904 a Royal Commission studied traffic in London. The speeds of various vehicles were taken. During off-peak periods a motor driven cab would travel at an average of 12 miles per hour. In 1996 the average off-peak vehicle speed was recorded as 10 miles per hour. They got an increase in the average speed when they introduced the congestion charge a few years ago, but now it is back down to almost the same level. The point being that the function and performance expected from a modern car is not so different from its 50 year old predecessor.

Communication capabilities and Internet speeds have, however, changed dramatically in the past 20 years, and people are not really interested in using old or slow equipment under any circumstances.

Enjoy the device you have – for now

The only conclusion we can make, considering the fast moving communications world, is to enjoy the device you have, as you will never see the like of it again. It is part of a technology evolution which is invoking changes at such a rate that previous generations of equipment are destined to be part of the urban rare metals mining programme within a few years.

More interesting is how we are being changed by this rapid movement of capabilities into our devices. When did you last dial a phone number from memory? Do you actually know where you have been or did you just follow the navigation system? Is your digital camera more reliable than your memory?

It looks like the user may become obsolete some day. Going back to the times when communication was cumbersome doesn't seem to be attractive. In conclusion, retro doesn't work with communications technology.

Privacy and data protection in the EU

Milon Gupta
Eurescom
gupta@eurescom.eu

Never before have private data been more important and more accesible than today. Private data are the basis for transactions in areas like banking, healthcare, and social networking. Driven by digitisation and the Internet, large amounts of private data are collected, stored and analysed by government bodies as well as companies. Legislature, regulators and industry in the EU are faced with the challenge of how to protect the citizens' personal data while at the same time enabling the free flow of data for the common good and protecting society from threats by criminals and terrorists.

The basis for citizens' privacy rights in Europe is Article 8 of the European Convention on Human Rights (ECHR). It provides a right to respect for one's ''private and family life, his home and his correspondence''. According to the case law of the European Court of Human Rights, gathering information for the official census, recording fingerprints and photographs in a police register, collecting medical data or details of personal expenditures and implementing a system of personal identification has been judged to raise data privacy issues. Any state interference with a person's privacy is only acceptable for the Court, if it is in accordance with the law, pursues a legitimate goal, and if it is necessary in a democratic society.

Revision of EU data privacy rules

Finding the right balance between the citizens' privacy and public as well as commercial needs is a major challenge in the current revision of the European Union's data protection framework. The EU data protection directive (95/46/EC), the central pillar of data protection in the EU, was published 16 years ago. Many of the technologies and services that impact data privacy today were not around then. Think of Cloud computing, social online networks, RFID chips, location-based services, mobile data communication, and powerful search engines that impact our privacy. On the Internet, citizens in Europe and worldwide are faced with a high level of cybercrime. In many cases, the challenges for the privacy of EU citizens originate outside of the EU.

The Voss report

On 15 June 2011, a report on the revision of the data protection framework, the Voss report, was adopted by the European Parliament. One of the key requirements is that EU data protection rules must also be applied outside of the EU. When personal data is transferred and processed outside the EU, ''it is imperative that data subjects' rights are fully enforced''. International data transfer procedures must be improved and ''ambitious core EU data protection aspects to be used in international agreements'' must be devised by the Commission.

Furthermore, the Voss report recommends that the updated data protection law should include ''severe and dissuasive sanctions'', including criminal penalties, for misuse and abuse of personal data. National data protection authorities should be given the necessary resources and be granted harmonised investigative and sanctioning powers, they say.

A major point of the Voss report is to strengthen the citiizens' rights to control what is done with their personal data. Companies should avoid erecting unnecessary barriers to the individual's right to access, amend or delete his/her personal data. In addition, the individual's consent to use of his data should be considered valid "only when it is unambiguous, informed, freely given, specific and explicit'', says the report.

From 4 November 2010 to 15 January 2011, the European Commission had already conducted a public consultation on the Commission's comprehensive approach to personal data protection in the European Union. The basis for the consultation was a Commission Communication on the issue, which was published on 4 November 2010.

Originally, the European Commission had planned to present a new proposal for the data protection rules by the end of 2011. Now it appears this will only happen in 2012. The delay indicates how difficult the decision-making process is.

Incidents related to data privacy

Some incidents this year have underlined the growing importance of data protection not only on regulatory but also on a technical level. In April 2011, Sony's PlayStation Network and Qriocity services were hacked and personal details, including credit card data, from approximately 77 million accounts were stolen by unknown intruders. The attack forced Sony to turn off the PlayStation Network for 23 days.

In October 2011, a different type of privacy-related event occurred. In Germany, police is allowed to secretly install a computer surveillance software ("Bundestrojaner" – Federal Trojan horse) on a suspect's computer in order to wiretap Internet telephony. The Federal Constitutional Court of Germany has ruled that the police may only use such programmes for telephony wiretappings. On 8 October 2011, the Chaos Computer Club, a German organization of hackers, found out that the software's functionality went far beyond wiretapping, thus violating the ruling of the constitutional court. In addition, the hackers identified a number of security problems with the implementation of the federal spyware.

Conclusion

Both incidents show that regulatory and technological improvements will be necessary to protect citizens' data without disrupting the legitimate use of private data by citizens, public authorities, and industry.

Improvements are particularly required in identity management and Cloud security. Industry and public authorities need to cooperate in order to reduce the risk of abuse of private data. For achieving this, Europe needs better law enforcement against cybercrime, further harmonisation and updating of regulation as well as technological measures like Privacy by Design.

Further information:
- EC data protection website
  http://ec.europa.eu/justice/data-protection
- A comprehensive approach on personal data protection in the European Union
  http://ec.europa.eu/justice/news/
  consulting_public/0006/com_2010_609_
  en.pdf
- Wikipedia article on PlayStation Network outage
  http://en.wikipedia.org/wiki/PlayStation_
  Network_outage

Privacy and identity management
Opportunities for telecoms network operators

Ricardo Azevedo Pereira
Portugal Telecom Inovação
ricardo-a-pereira@ptinovacao.pt

In today's networked world, identity and privacy have become of crucial importance. Most of actual online services require identity-related data in order to function, further augmenting the already growing concerns regarding privacy, as well as the usability and general sustainability of current identity solutions. In response to this, Identity Management (IdM) and Privacy Enhancing Technologies (PETs) are more than ever seen as essential parts of systems and of critical importance. This article is based on a Eurescom study which looked into the opportunities which privacy and identiy management provides for telcos.

Telecommunication operators' vast customer base, existing infrastructure and experience in dealing with large scale identity management (e.g. mobile SIM cards) give telcos an advantage towards competitors. It is therefore essential for telcos to understand how best to take advantage of these emerging fields. The Eurescom Study P1953, "New opportunities for telecommunication operators on privacy and identity management" identified, described and evaluated a variety of potential business segments which are closely intertwined with IdM & PETs.

Major driving forces vs roadblocks

With telcos in mind, there are several major driving forces from a strategic point of view:

- The need for the user to control his private information, to avoid leakage of information that may result in personal damage and uncontrolled incidents.
- The possibility for telcos to establish services in new arenas, take positions in new value chains and with new partners targeting new business opportunities.
- With many customers, telcos are viewed as reliable business partners, by most stakeholders.
- The mobile phone could be used as a facilitator and enabler for any kind of electronic purchase, and more generally for management of the user's digital life.
- As e-health, financial and e-government services become pervasive in the individuals' life, the mobile phone and telco servers could become privacy-conscious repositories for vital information.

There are, however, several roadblocks that may prevent early adoption of those technologies. Such roadblocks are both technical and non-technical issues which will require a multi-disciplinary approach to be solved, taking into account human, legal, economic, and technical perspectives. The figure shows how the roadblocks identified within P1953 can be lifted with concrete actions.
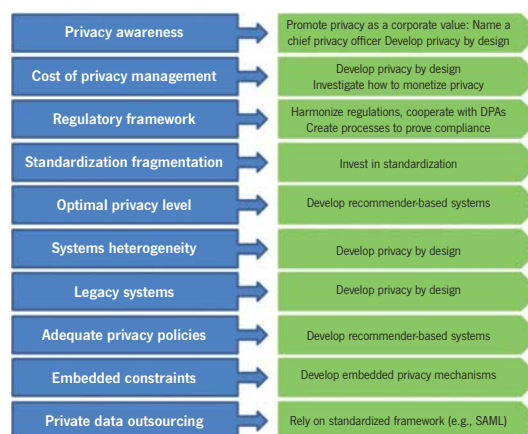

Figure: Roadblocks and recommendations

Promising segments overview

The analysed segments include different areas, from Financial to Digital Home, M2M or e-Health and e-Government. The evaluation on potentially successful scenarios and business applications or services followed the Chesbrough model for open innovation. According to this evaluation, the segments that look more promising were the financial, the e-Government and the Enterprise segment. Moreover "Strong Authentication as a Service" was identified as a transversal service. The list below provides a short overview on the chosen segments and its relationship with IdM and PETs.

- The Financial segment incorporates mobile services to facilitate money transactions or payments, account overview, and other general banking services where a high level of security and/or authentication is required.
- The e-Government segment includes digital interactions and information exchange in a citizen-to-government (C2G) way. Such services apply to very different contexts, authentication levels, and privacy to protect the citizen's affairs from public insight. They heavily rely on IdM systems that should be consistent and interoperable.
- The Enterprise segment focuses on the requirements imposed by foreseen changes from a traditional closed enterprise to an open paradigm. Telcos may reuse authentication and authorization services to integrate easily with the already in place mechanisms, simplifying the access, i.e. network access based on enterprise authentication/authorization mechanisms.

The next steps are important

Technologies for identity and privacy management are disruptive and may significantly impact a telco's business. Understanding the technological roadmaps and users' expectations is at the front line for telcos to target the integration of these technologies in their networks. Four other aspects, including operational, architectural, evangelistic and commercial aspects, are of special importance and need to be taken into consideration in a combined way. From the commercial point of view it is essential to adopt a business model such as a fixed-fee-per-user-per-month billing model or a step based approach with a number of inclusive OCSP (Online Certificate Status Protocol) requests per month, mixed with a clear definition of what assets and already-in-place services can be presented commercially.

Some of the involved technologies are not mature enough for full deployment, which means telcos should start introducing privacy technologies at devices and services platforms and move toward the core-network as it matures. At the same time, the adoption of an architectural approach to privacy infrastructure design instead of an ad-hoc manner is vital. Only a coordinated approach, based on different perspectives, domains and actual actions, can leverage telcos to a top position in terms of identity and privacy service offerings, creating new business opportunities and overcoming the dreaded "just-a-bit-pipe" scenarios.

Stronger rights for citizens and data protection authorities

Interview with Peter Hustinx on data privacy in Europe

The rapid pace of technological progress and the development of personalised services are posing serious challenges to European citizens and regulators. Eurescom mess@ge editor-in-chief Milon Gupta interviewed the European Data Protection Supervisor, Peter Hustinx, on the challenges to data privacy in Europe, and how regulators and citizens should respond to them.

Which are currently the main issues in regard to data privacy in Europe?

Our societies now depend on the good use – and thus also the well functioning – of various kinds of ICT. Internet and mobile applications are playing a crucial role. This leads to many new issues, including the widespread tracking and tracing of individual behaviour, without sufficient knowledge and control of those involved. We also discover how vulnerable we are for malicious attacks. It is therefore in everybody's interest that we make our information society more robust, more responsible and more trustworthy. Data privacy is in that sense only part of a much larger issue.

How well protected are private user data in today's cloud services, and what could cloud service users do to increase their privacy?

As a recent study for the European Commission by RAND Europe has shown, the current landscape for cloud computing is still characterised by a number of challenges for security, privacy and trust. Some of these challenges may be addressed by regulatory measures, but many others require a greater accountability of both providers and users of cloud services. Consideration of privacy and security is now too often an afterthought or treated separately, and it is often difficult to negotiate specific security terms with cloud service providers. This should clearly change. Users and providers should be more alert, and services offered to the public should be bound to minimum standards.

What are the main challenges for the revision of the EU data protection framework?

The main part of the current EU data protection framework – the Data Protection Directive 95/46/EC – is now showing its age and should be modernised to face the challenges of new

European Data Protection Supervisor Peter Hustinx

technologies and globalisation. The emphasis should be put on ensuring that the present principles are more effective in practice. This will require stronger rights for data subjects, more responsibility for organisations, and stronger enforcement powers for data protection authorities. At the same time we need to ensure that the new framework will apply in all EU policy areas, including law enforcement, and that the current unhelpful diversity is reduced.

How much do data regulations in the EU member states diverge, and what should be done to harmonise them?

The current Directive aimed at greater harmonisation, but left a margin of manoeuvre to member states. After 15 years this has led to considerable diversity and complexity among member states, not including some resulting from inaccurate implementation. This is bad for the development of the internal market, but also for effective data protection. The new framework should therefore in any case reduce unhelpful diversity and clarify the scope for some remaining diversity. This would require a more detailed Directive or a Regulation, but also effective arrangements for close cooperation and greater consistency between national supervisory authorities.

To what extent are data of European citizens and companies protected that are stored at organisations outside of Europe?

The Directive provides that EU data protection law applies to the processing of personal data where the responsible organisation, the Controller, is established in an EU member state. This means that EU data protection law continues to

apply where a controller in the EU transfers data outside the EU, for instance to a service provider in a third country, except where the responsibility is also passed on to the recipient in a third country. For both cases, the Directive provides a few additional safeguards to ensure adequate protection. This may require a special contract or another instrument such as Binding Corporate Rules.

What is the economic impact of data protection?

Data protection has an economic impact, certainly at a scale where it is now relevant for the well-being of our information societies. In that context, the attention has gradually shifted to the need for data protection as a condition for trust – both online and offline – and economic development. A growing need for compliance with data protection will probably also lead to growing demand for privacy professionals and for privacy products and services. At the same time, it remains important to avoid unnecessary burdens and to simplify relevant rules where possible. All this plays a crucial role in the review of the current legal framework.

What is the single most important data protection issue you would like to see solved in the next five years?

My single most important wish is that we are successful in achieving a more effective EU legal framework for data protection by 2015. This is just in time to meet the ambition for smart, sustainable and inclusive growth that is at the heart of the EU 2020 strategy.

The European Data Protection Supervisor is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. It does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy; and
- co-operating with similar authorities to ensure consistent data protection.

Website: www.edps.europa.eu

Privacy by Design
An industry perspective on the challenges and opportunities of privacy

Aljosa Pasic
Member of the EOS Board
of Directors
Aljosa.Pasic@atos.net

Privacy issues have far-ranging implications, both for citizens and for industry. This article explores some of them from an industry perspective, based on the position of the European Organisation for Security (EOS), with a particular focus on the concept of Privacy by Design.

Privacy concerns of European citizens are increasingly subject to public discussion, both for offline scenarios in the real physical world, e.g. security checks at the airport, and online scenarios in the virtual world of the Internet. In the cyberworld privacy concerns are especially important because of their dynamic development in combination with the rapid technology evolution.

Trade-offs between risks and benefits

Since the introduction of location-based services, these concerns extend also to privacy risks related to location or presence. In both worlds, privacy value contains factors and variables that reflect the trade-offs an individual has to make between benefits and risks in having his or her private data being used. Benefits could be, for example, gain of comfort, increased functionality, or discounts; risks may include misuse or manipulation of private data.

A similar trade-off analysis is done by organizations, whether they act as data controller or data processor. With the increasing regulatory pressure it became common to perform detailed analysis of privacy value that takes into account cost (financial, effort), convenience in compliance management alternatives, benefits (saving time or money), security, transparency, trust in a particular partner organization, trustworthiness of the supporting technology, mechanisms that enable provision of services or data transfer by/to a third party, the amount of control over client data, etc. This complexity in privacy value assessment is often making it difficult to address privacy problems in a systematic way.

In the past decade, there was a lot of emphasis on regulations and compliance-driven approaches to privacy and data protection. The list of related regulations is long: Directive 95/46/EC, Regulation (EC) Nr. 45/2001 applicable to data processing by EU institutions and bodies, Directive 2002/58/EC on privacy and electronic communications, Framework Decision 2008/977/JHA on data protection in the area of police and judicial cooperation in criminal matters and Directive 2009/136/EC (amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

In addition to regulation, concepts such as "privacy by design" emerged as a way to deal with privacy issues. Yet, privacy concerns still need to be transposed into specific, precise and non-ambiguous technical requirements if they are to allow the security industry to competitively design and develop privacy-compliant solutions and services. The Privacy by Design (PbD) concept should, at its turn, be better detailed in order to allow for its practical implementation in concrete cases.

Challenges for European industry

When developing security solutions compliant with privacy and data protection requirements, suppliers have to face several challenges, which impact the competitiveness of the European industry:

- Regulations are pretty general; for instance, the "Proportionality Principle" is sometimes interpreted very differently from one country to another with the potential creation of market distortion;
- National guidelines are sometimes incompatible with each other;
- Compliance evaluation of a new product or service, when requested, is a very lengthy process, often on a case-by-case basis, demanding substantial investment of time and resources.

To support EU industry in facing these challenges, we need sufficiently precise and consistent privacy and data protection requirements

that can be used in developing PbD in an unambiguous fashion. These requirements should be sufficiently homogenous across the European Union, thus avoiding a duplication of needed approvals, evaluations and efforts. They should take also into consideration the specifics of the security of systems, software and services as well as the physical security of citizens, goods and infrastructures.

Demands and initiatives by industry

The European Organisation for Security (EOS) is currently preparing a "Charter for Security Solutions and Services compliant with Privacy and Data Protection Requirements" to be proposed for voluntary endorsement by EU technology and service security providers, starting from EOS members.

This EOS initiative shows that European industry is seeing investments in privacy-enhancing technologies as a question of competitive advantage. However, trade-off analysis is extremely complex, as it involves multiple stakeholders and deals with dynamic intangible issues such as trust or context. At EOS we believe that a new approach, which includes a public-private dialogue, is needed to support regulatory decision makers and to introduce new alternatives in dealing with privacy risks.

The European security industry needs clear requirements and criteria for the development of Privacy by Design (PbD) solutions, but also assessment and validation criteria on what can be labeled as PbD.

Proposals by EOS

EOS has therefore proposed a number of measures to the European Commission and the National Data Protection Agencies, which include:

- Review the current framework on the basis of a technology-neutral and, as much as possible, commonly agreed and self-regulatory approach. Principles and provisions must be flexible so that people who are creating new programs, products and services understand

Android security
Securing Android based devices

how to accomplish their business goals while also protecting individuals' privacy.

- Tackle privacy from a global perspective with respect to enforcement and cross border cooperation including the use and protection of personal data. Discussions and considerations should be targeted beyond the EU 27.
- Link foundational privacy protection goals on concrete requirements. Any requirement should at least satisfy the conditions of being simple, easily comprehensible and applicable in practice.
- Pursue the effort of harmonising the privacy and data protection regulations inside the EU first, and then at international level.
- Use the research programmes FP7 and later Horizon 2020 to initiate studies on concrete approaches to Privacy by Design and data protection, including tests of their viability. In this way, privacy concerns can be met upfront in a scalable and flexible manner. The Framework Programme for Security Research provides the benefit of having all types of stakeholders cooperating on innovative approaches.
- Develop, when needed, agreed PbD evaluation criteria in order to significantly increase the efficiency of the design and the validation of products and services. Such an approach would need to be extended as much as possible across Europe.

Furthermore, EOS also urges all political stakeholders to promptly address the need to revise the strictly political and legal aspects that the collection, storing and handling of data, including data transfers to third countries, involves.

Conclusion

Privacy can be an opportunity for European citizens and industry alike. What we need is a public-private dialogue on the specifics of harmonised and consistent EU-wide regulation and the development of effective Privacy by Design.

For more information about the European Organisation for Security and its positions and initiatives on privacy please visit the EOS website at www.eos-eu.com

Dr. Matthias Baumgart
Deutsche Telekom Innovation Laboratories
Matthias.Baumgart@ telekom.de

Our daily lives have become more and more influenced by smartphones and their tremendous capability to exchange information, play games, buy products, book services or enter the corporate network. One of the most popular operating systems on smartphones is Android. This article presents some of the results of a Eurescom study on how to increase the security of Android-based devices.

Android – A popular target

Android has come up as an open smartphone platform which offers the possibility to extend the platform with apps or even modifications on operating system level. Android quickly gained popularity among smartphone developers and

continues to evolve further from a platform for smartphones to a platform for netbooks, tablets and also to be integrated into home appliances. The widespread use of the Android platform increases also its appeal as a target for attacks. Attackers use the open framework of Android and seek for potential weaknesses that can be exploited to gain profit.

This profit may not only reside in direct financial profit but also in reputation in finding new weaknesses.

Often the goal is to jailbreak Android devices, which means to gain super user rights on the device. Although the intention is to give the user the freedom that he usually doesn't have on the device and for instance gain access to other app-markets than the Android market, this also opens the door for further attacks, as built in security mechanisms are bypassed.

Potential risks inside Android

Some of these attacks against Android, like the malware that sends SMS to premium-rate numbers, gained public attention and show the need for enhanced security in Android.
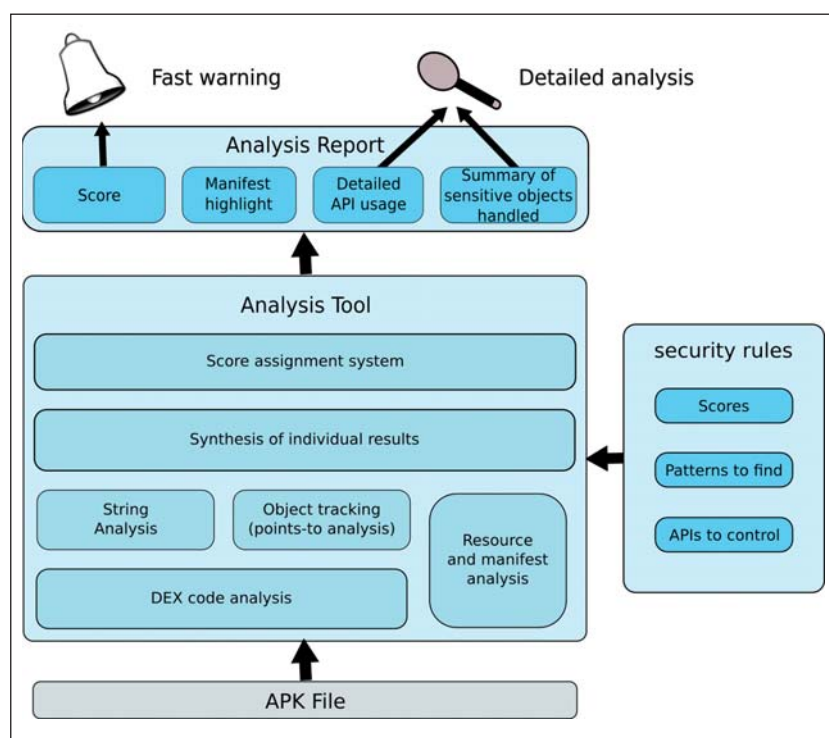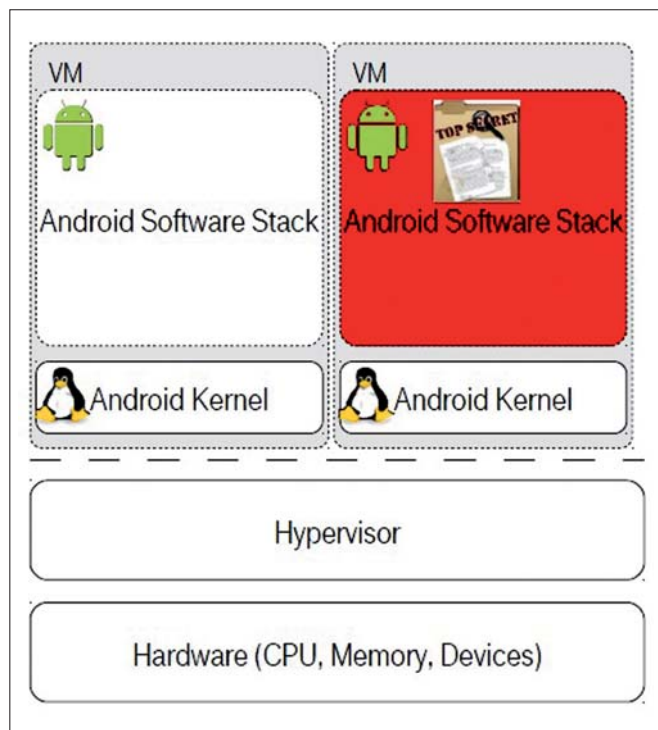

Figure 1: Android bytecode analyser

Figure 2: Running two Android instances on a secure Microkernel

Within the Eurescom Study P2057 'Android OS Security Issues – the operators' view' the security risks residing within Android were analyzed and appropriate countermeasures were proposed by the partners of the study.

Many of the potential risks inside Android can be exploited by malware. Often this malware uses security flaws that have not been fixed by a firmware update or benefits from the fact that the firmware update has not yet been installed. Other malware uses the fact that users are not aware of the security risks when granting an app access to the SMS stack or to other resources on the device.

One major countermeasure against several threats is to raise the user awareness about these threats. The operators can also play an important role in this issue by educating the user or providing additional security services on the device. This includes informing the user about possible privacy issues of Android based smartphones as Google forces the user to register with a Google account and is not forced to fulfil the privacy regulations of the European Union.

Other common possibilities to mitigate the risks by malware are the installation of a malware detection system or an anti virus software on the device, the provisioning of regular firmware updates and the removal of malicious software from the device and the market.

Innovative new methods will help to mitigate the risk of these attacks. For instance methods like clone detection and bytecode analysis of apps as shown in figure 1 will help to detect malware and secure kernels like a secure microkernel approach will ensure secure separation of services or even Android instances as shown in figure 2, and reducing the risk of jailbreaking devices.

Securing Android is a joint effort

Providing regular firmware updates is a good example why a collaboration and joint effort of Google, the device manufacturers and the operators are needed to achieve an appropriate level of security. As proprietor of the Android system it is primarily the responsibility of Google to provide such an update. However, each model often has a slightly different firmware. and vendors of the devices have a responsibility to ensure that their device-specific firmware stay up to date. Finally the operator can help to ensure a timely update by informing the customers and providing help services for the update.

Furthermore, the exchange of security related data between operators helps to mitigate the risks of new vulnerabilities and attacks against Android based systems.

Finally, a joint approach of European operators towards Google and the device manufacturers advocating the security issues and privacy concerns of their customers could be the last missing piece of the strategy puzzle towards a secure open Android platform.

NEM Summit 2011

Implementing the Future Media Internet

Halid Hrasnica
Eurescom
hrasnica@eurescom.eu

Peter Stollenmayer
Eurescom
stollenmayer@eurescom.eu

This year the NEM Summit took place in Torino from 27-29 September 2011. It was the fourth NEM Summit which focused on the whole innovation chain, leading from ideas towards the future media Internet to the actual implementation of it. More than 300 participants had registered for the Summit and discussed related technological, implementation and business issues. The Summit was accompanied by an exhibition where about 40 projects, organisations, and individuals presented recent research results and showed artistic achievements by applying NEM technologies.

This year's NEM Summit was clearly focused at social and user aspects of the electronic media. This was also reflected in the NEM-Art contest, which was performed for the first time in such a Summit.

One of the Summit highlights, besides the presentations of papers by 36 highly recognised speakers and the exhibition, was an art contest in which 16 NEM-Art exhibitors took part. The NEM Summit was organised by the European Technology Platform (ETP) on Networked and Electronic Media (NEM) under the aegis of the European Commission. This year it was hosted by Politechnico di Torino with support from Telecom Italia and further local organisations.

The NEM Summit brought together a unique group of international experts: representatives of the NEM community from Europe and worldwide, major manufacturers and service compa-

Opening speech by NEM chairman Jean-Dominique Meunier from Technicolor

nies, start-ups and SMEs, research centres and institutions, industry associations and groups as well as standardization and regulation bodies.

The Fourth NEM Summit 2011 was dedicated to the theme ''Implementing Future Media Internet''. It included 25 papers, selected by the Technical Programme Committee out of 56 submitted papers, and several invited papers and keynote talks. The main topics addressed at the event were social media and user media, which again underlines the user-centred focus of this Summit.

NEM Summit 2011 in numbers

- About 350 delegates
- 18 sponsors
- 23 project demos
- 16 NEM-ART award exhibits
- 4 collocated workshops, NEM General Assembly and NEM Expression of Interests
- 56 papers submitted of which 25 were selected
- 6 papers selected for publishing in Elsevier Computer Communications
- 7 keynote speeches

The conference

The conference was inter alia opened by Neelie Kroes, Commissioner for Information Society and Media and by Megan Richards, Director of DG Information Society and Media, though both only via video message.

Gabriela Ella from Telekom Italia stressed in her keynote speech that currently only 50 applications account for more than 75% of the Internet traffic. This emphasises the high importance of Future Media on the Internet.

In the following seven technical sessions the participants discussed various issues related to the Future Media Internet. Several topics were discussed, particularly societal and user related issues related to the Future Internet. Finally the users have really been put in the centre of the discussions and solutions.

The exhibition

The Summit included a well targeted exhibition with over 23 stands from projects and organisations related to the future media Internet. Projects from the European R&D Framework Programmes had a good part of the exhibition, but also several demos from the CELTIC Initiative were present. Amongst the FP7 demos was the

TA2 stand at the NEM Summit 2011

Integrating Project TA2 (Together Anywhere, Together Anytime), which showed how geographically separated families and friends can keep a feeling of togetherness through applying appropriate ICT services.

A novelty were the 16 NEM-Art exhibits which gave an artistic impression about future media and ICT and how modern media technologies can successfully support the artists' creativity. Amongst them was the award winning exhibit "Isabella: the secret recipes", an edutainment game, which illustrates the work of alchemist women in ordinary people's lives during the 16th century in Venice.

The workshops

The NEM Summit 2011 included several colocated workshops:
- NEM Sandpit workshop
- Search computing and social media workshop
- JUMA workshop
- TA2 workshop on managing ICT projects in FP7 – exchange of best practices

The TA2 workshop on "Managing ICT projects in FP7 – exchange of best practices" was a follow-on of several similar workshops organised by Eurescom to share experiences how to best manage collaborative R&D projects in the ICT area.

About the NEM Initiative

Set up in 2005, NEM is a European Technology Platform dedicated to Networked and Electronic Media. With more than 800 members, it is a large-scale European industrial initiative to accelerate the pace of innovation through convergence between content creation, audiovisual, telecommunications and broadcasting, as well as information technologies sectors and to place the European industry at the forefront of the information era. NEM brings together industrial players and research institutes from more than 30 countries.

More information about the NEM Initiative is available at http://www.nem-initiative.org.
The slides of the TA2 management seminar can be downloaded from http://www.ta2-project.eu/NEM-Summit-2011/seminar2011-agenda.html

Net!Works General Assembly in Brussels

Linking ICT with application areas

Uwe Herzog
Eurescom
herzog@eurescom.eu

Net!Works

The 7th General Assembly of the European Technology Platform Net!Works took place in Brussels on 5 October 2011. It attracted about 70 participants. Besides reports about the platform's activities and achievements, the presentations addressed three major topics: Informing about the progress towards Horizon 2020, highlighting the link between ICT and several application areas, and to inform about the progress of the Future Internet Public Private Partnership (PPP) activities. Furthermore, Net!Works members also successfully elected the new Net!Works Steering Board for the period 2012-13.

Net!Works has now more than 800 members

Net!Works chairman Werner Mohr informed in his opening speech informed about the activities during the last year. A major milestone has been the change of the platform's name from eMobility to Net!Works. This was done in order to reflect the widened scope of the platform which now also addresses optical networks aspects, and in order to distinguish from the term e-mobility, which is increasingly used by the electric car industry. In order to address the optical sector a close liaison with the Photonics21 platform has been set up. The growth of Net!Works membership has continued at a high pace and resulted in currently 807 members.

Early information about Horizon 2020

Rudolf Strohmeier, Deputy Director General at the European Commission DG Research and Innovation, explained that Horizon 2020 will be aligned with Europe 2020. Budgets will be made available to Research & Innovation, but also for demonstration projects and prototypes. At the moment, the lead time for new products is considered being too long, and therefore Horizon 2020 will improve the integration of research and

Luis Rodriguez-Rosello from the European Commission spoke about the role of ICT in Horizon 2020

innovation. In parts of the programme, cooperative research will become integrated with application areas. This intends to ensure that ICT research is closely linked with the societal

challenges. Nevertheless, it is also planned to have a dedicated budget for funding longer term concept development in ICT, e.g. for next generation systems. The Commission's proposals for the 2014-2020 framework foresees a 80 billion euro budget for Research & Innovation. Complementing that speech, Luis Rodriguez-Rosello from the Information Society and Media DG at the EC explained the role of ICT in Horizon 2020. While Horizon 2020 is still a few years ahead, Andrew Houghton, also from the Information Society and Media DG, presented more current matters with some information about FP7 Workprogrammes 2011-12 and 2013.

A political view from an MEP

Malcolm Harbour, Member of the European Parliament, addressed the GA participants during the lunch break with his ideas on drivers of innovation in the single market. In this very inspiring speech, Mr Harbour informed about the opportunities for businesses arising from the single

Malcolm Harbour, Member of the European Parliament, at his lunch speech on drivers of innovation in the single market

The newly elected Steering Board.

European market and gave his view on where there could be business opportunities for ICT in other sectors.

Opportunities for ICT in application areas

A number of presenters from several application areas spoke about the challenges in their area, and pointed out where ICT in their view could help to overcome them. Paul Verhoef, Head of Unit ''Research and Innovative Transport Systems'' at DG Mobility and Transport, spoke about the needs for ICT and in particularly telecoms in the transport sector. The main challenge in the transport sector is to break the transport system's dependence on oil without sacrificing its efficiency and compromising mobility. Avoiding the need to travel, shifting to more efficient transport modes and improving transport modes are all aspects where ICT will be required for addressing them. Further speakers presented their views on ICT for Smart Grids, and ICT for enhancing governance and democracy.

Election of the new Net!Works Steering Board

During the General Assembly the members also elected the new Net!Works Steering Board for the period 2012-13. There have been a few changes in the composition. The list of elected organisations is given in the box.

Net!Works

Net!Works Steering Board organisations for the period 2012-13

Industry group members
- ADVA AG
- Alcatel-Lucent
- ATOS
- Deutsche Telekom
- DoCoMo Communication Laboratories Europe
- Engineering ingegneria informatica s.p.a.
- Ericsson AB
- Intracom S. A. Telecom Solutions
- NEC Europe
- Nokia Siemens Networks
- ST-Ericsson
- Telecom Italia
- Telefónica
- Telenor ASA
- Thales Communications SA

Research group members
- Centre Tecnologic de Telecomunicacions de Catalunya (CTTC)
- IST – Tech. Univ. Lisbon
- ITI - Instituto Tecnologico de Informatica
- Tecnalia
- Waterford Institute of Technology

SME group members
- Beacon Tech Ltd.
- GOWEX
- InterInnov
- Sigma Orionis

More information about the GA and the presented slides are available for download on the Net!Works website at www.networks-etp.eu

Infrastructures, services and the user
Future Internet Week in Poznan

Milon Gupta
Eurescom
gupta@eurescom.eu

The second Future Internet Week of 2011 was held in Poznań, Poland, from 24 to 28 October 2011. The participants from all over Europe and abroad met at the campus of the Poznań University of Technology on the banks of the Warta River. They came to join the numerous sessions and network in the breaks or learn about the latest project results in the exhibition.

Due to the large number of parallel sessions, it was impossible to get a complete overview of what happened at the event. Thus, this report cannot claim to give a full picture of the Future Internet Week, but rather a few subjective glimpses and observations, mainly on the the Future Internet Assembly, which ran from Tuesday to Wednesday.

Commission troika at the opening session of the Future Internet Week (from left): Megan Richards, Director of the Converged Networks and Services Department, Information Society and Media DG; Michael Ralph, Adviser to Director General, Directorate General for Regional Policy; Mario Campolargo, Director of the Emerging Technologies and Infrastructure Department, Information Society and Media DG.

Future Internet Assembly

In the opening session of the Future Internet Assembly, Megan Richards, Director Converged Networks and Services at the Information Society and Media Directorate-General, presented the European Commission's view on the deployment of Future Internet research results and how this should lead to innovation.

Ms Richards particularly stressed the importance of understanding the needs of regional and local actors as well as adopting a comprehensive and integrated approach. In this context, she mentioned Smart Cities as an excellent application field for this integrated approach, which would break down silos between domains such as buildings, transport, energy networks and ICT.

In order to facilitate this, the Commission plans to introduce a new instrument called Connecting Europe Facility (CEF), which is meant to combine market-based instruments and direct support by the EU to optimise financing impact for supporting cross-sector innovation in transport, energy, and digital infrastructures. In order to get there, she argued that the European R&D community should move from testing innovative

Jonathan Cave, RAND Europe, talking about economic impacts of the Future Internet at the Future Internet Week 2011

ideas to piloting realistic solutions to deliver Future Internet-related innovations in the 2020 timeframe.

Economic impact of Future Internet PPP

Jonathan Cave from RAND Europe presented results of the FI3P project (www.fi3p.eu) on the potential economic and longer-term societal impacts of the Future Internet PPP. He considers the Internet economy a leading factor for Europe's economic recovery. Currently the Internet economy adds 4.1 percent to the EU's gross domestic product . He expects this share to grow by a factor of seven. He predicts that the Future Internet PPP will raise the Internet economy's contribution to GDP by 5.7 percent.

Bolesław Szymański, Professor of Computer Science at the Rensselaer Polytechnic Institute in Troy, NY, presented his vision of a People's Internet. His basic assumption is that the Internet is transforming social interaction.

He identified a number of social network transformation issues. This includes the evolution of opinions and ideas via the Internet and the issue of how trust is established on the Internet. An important question Prof. Szymański asked in this context is, how the existence of information networks changes the dynamics of human interaction.

Impression from the demonstration evening.

Another transformation enabled by the Internet is that humans can function and work together as networked sensors. Unfortunately, the extremely brief questions-and-answers rounds after each rather long presentation did not allow a meaningful discussion between panel members and the audience.

It is somehow strange that despite all the talk about innovation and social transformation, presentations at Future Internet events are still run like 19th century university lectures.

Professor Bolesław Szymański presenting his ideas on social network transformation at Future Internet Week 2011

Parallel sessions

My personal impression of the parallel sessions and the feedback I received from colleagues is that in general, meaningful discussion was rather neglected in favour of having too many presentations with too many slides. Most of the parallel sessions on specific topics like the Trust Framework for Future Internet Services and Infrastructures, the Mobile Cloud, and the Future Internet Research Roadmap were lacking a structured, and deeper discussion involving the audience. Instead, usually a row of presenters were hurrying through their presentations, which were not always logically connected to each other or to a common theme.

Infrastructure meets user

Fortunately, some sessions did enable a more interactive discussion. One of those was the session "When infrastructure meets the user", moderated by Dr Petra Turkama from Aalto University, who coordinates the CONCORD support action within the FI-PPP, and Jarmo Eskelinen from Forum Virium Helsinki, who is Vice-President of the European Network of Living Labs (EnoLL). The panel consisted mainly of representatives from

Parallel sessions in the lecture hall

the FI-PPP usage area projects and the FI-WARE core platform project, who gave brief presentations – without slides! – on what their respective projects are doing in regard to infrastructures and users. The FI-PPP usage area presentations were complemented with a presentation on ICT infrastructures for emerging e-health services, given by Dr Cezary Mazurek, Head of the Network Services Department at the Poznan Supercomputing and Networking Center.

One of the interesting questions discussed by the panel and the audience was how to approach user-driven innovation, and who these users are. While the discussion mainly focused on business users and end users, Nick Wainwright from HP reminded the audience not to forget one important user group, namely the developer community.

Conclusion

Although the Future Internet Week did not deliver any earth-shattering new insights, it was a useful get-together of the European Future Internet community. It enabled, for example the FI-PPP, the Internet of Things (IoT), and the Future Internet Research and Experimentation (FIRE) communities to have joint meetings and to get an overview on the progress of the different European Future Internet research areas.

The considerable participation of representatives from other regions of the world, particularly Latin America and Asia, indicated that Europe's Future Internet research has global relevance. It will be interesting to see at the next Future Internet Week, which will be held under the Danish EU Presidency in Aalborg in May 2012, how much progress, particularly in the Future Internet PPP, will have been made by then.

Further information on the Future Internet Week is available at www.fi-poznan.eu

TRILOGY receives Future Internet Award

Copyright by PSNC 2011

Award session at the Future Internet Week 2011 (from left): Phil Eardley (Trilogy project), Willie Donnelly (ceFIMS coordinator), Megan Richards (European Commission), Robert Szabo (Judging Panel)

FP7 project TRILOGY, which has developed a long-term solution to Internet traffic congestion, received the Future Internet Award at the Future Internet Week in Poznan, Poland, on 28 October 2011. The EU-funded project received the award for its outstanding contribution to the Internet architecture and protocols, which could help provide Europeans with faster, more reliable Internet connections.

Specifically, TRILOGY has developed the Multi-Path Transmission Control Protocol (MPTCP), an extension to standard Internet TCP that enables data to be transmitted from one network node to another via multiple network paths at the same time, an algorithm for multipath routing to take advantage of multi-homing at endpoints and "congestion exposure" extensions to the Internet Protocol (IP) to monitor Internet congestion. In combination, they will enable a more resilient, more flexible and more cost effective Internet.

The results of the TRILOGY project are already being taken up by the ICT industry and are integrated into open source and commercially available operating systems to ensure that Internet connections become more resilient and flexible for all users.

One of the 11 consortium partners from Belgium, Finland, Germany, Greece, Spain, UK and the US is Eurescom, which contributed to the effective management of the project and the dissemination of project results. After winning the Future Internet Award already in 2009 with Panlab, this is already the second time Eurescom is in the Award-winning project team.

TRILOGY website: www.trilogy-project.org

News in brief

First joint EU-US cyber security exercise

Cyber Atlantic 2011: ENISA's Executive Director, Professor Udo Helmbrecht (left), and representatives of the European Commission and the Department of Homeland Security.

The first joint cyber security exercise between the EU and the US was held in Brussels on 3rd November 2011. It was supported by the EU's cyber security agency ENISA and the US Department of Homeland Security. The day-long table-top exercise ''Cyber Atlantic 2011'' used simulated cyber-crisis scenarios to explore how the EU and US would cooperate in the event of cyber-attacks on their critical information infrastructures.

In the first scenario, a targeted stealthy cyber-attack attempts to exfiltrate and publish online secret information from EU Member States' cyber security agencies. The second simulation focuses on the disruption of supervisory control and data acquisition systems in power generation infrastructures.

More than 20 EU Member States were involved in the exercise, 16 of them actively playing, with the European Commission providing high-level direction. Cyber Atlantic 2011 is part of an EU-US commitment to cyber security which was made at the EU-US summit in Lisbon on 20 November 2010.

The aims are to tackle new threats to the global networks upon which the security and prosperity of Western societies increasingly depend.

The exercise draws on lessons learned in the first pan-European cyber security "stress test" exercise, Cyber Europe 2010, which was facilitated last year by ENISA. ENISA's role involves supporting EU Member States in organising cyber security exercises and formulating national contingency plans as well as providing good practice guides and seminars.

Lessons learned from Cyber Atlantic 2011 will be used to plan further potential joint EU-US cyber exercises in the future.

http://www.enisa.europa.eu

## International body against cybercrime launched

In early July 2012, the International Cyber Security Protection Alliance (ICSPA) was set up in London to fight cybercrime on a global scale. One of the primary goals of the new body is to provide help to the countries that need most assistance, such as China.

The new body unites governments, international businesses and law enforcement agencies, including Europol. Major security companies such as McAfee and Trend Micro have also signed up. Funding for the alliance is expected to come from the EU and a number of governments.

https://www.icspa.org/

IBM produces first brain-like chip

IBM has developed a microprocessor which it claims comes closer than ever to replicating the human brain. The chip was designed in a project called SyNAPSE and is capable of reshaping its connections as it encounters new information, similar to the way biological synapses work in the human brain.
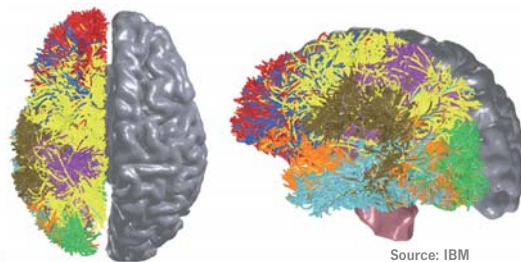
Source: IBM

The IBM research team led by Dharmendra Modha believe that by replicating this function of the brain, the technology could start to learn. Cognitive computers may eventually be used for understanding human behaviour as well as environmental monitoring. The researchers are also trying to recreate other aspects of the mind such as emotion, perception, sensation, and cognition by analysing the construction of the brain.

The SyNAPSE system uses two neurosynaptic computing chips with 256 computational cores each. These cores are the electronic equivalent of neurons. One chip has 262,144 programmable synapses, while the other contains 65,536 learning synapses.

In humans and animals, synaptic connections between brain cells physically connect themselves depending on our experience of the world. The process of learning is essentially the forming and strengthening of connections.

A machine cannot solder and de-solder its electrical tracks. However, it can simulate such a system by making important input signals stronger, and less important signals weaker.

IBM and its academic partners have been awarded 21 million dollar by the US Defense Advanced Research Projects Agency (DARPA) to continue their work on the SyNAPSE project.

http://www-03.ibm.com/press/us/en/pressrelease/28842.wss

ICT and the next billion people

Milon Gupta
Eurescom
gupta@eurescom.eu

In October 2011, the seventh billion inhabitant of this planet was born, according to the United Nations. In the twelve years since 1999, world population has grown by one billion. The UN forecasts the next billion by 2027, and by 2046, it is estimated that nine billion people will inhabit the Earth. This rapid growth of world population has tremendous social and economic implications for future human development, and ICT will play an important role in this development.

UN Secretary-General Ban Ki-moon (centre) and students in New York on 24 October 2011, celebrating that world population has reached 7 billion.

Most of the population growth takes place in developing countries, while the population in developed regions grows only slowly. The fastest growth takes place in Africa, while Asia will continue to have the largest share of world population in this century. In India alone, 51 babies are born every minute. Looking at the Worldometer population clock at www.worldometers.info makes you dizzy, as the numbers indicating real-time population growth are ticking away so fast.

This fast growth of world population raises questions about the availability and distribution of resources. Will there be enough food, clean water, and energy for 10 billion people on this planet in the not-so-distant future? At the moment, developed countries are consuming the largest share of global resources. What will happen, if developing countries catch up? Will economic development in Africa and Asia slow down population growth? Or will it just lead to a faster depletion of natural resources and an increasing fight for access to these resources?

Estimated and projected population by major area, medium variant , 1950-2100 (billions)

ICT and the Millennium Goals

In order to improve the quality of life for the growing world population in developing countries, the United Nations had defined eight development goals, the so-called Millennium Goals, which are to be achieved by 2015. Looking at these goals from an ICT perspective, it seems information and communication technologies can make a

significant contribution in achieving some of them.

Goal 1 is to eradicate extreme poverty and hunger. ICTs may not appear to be the first priority when it comes to this goal. However, access to information can significantly increase the economic situation of people and businesses in developing countries. Think of farmers who can increase their crop yields and better sell their harvest thanks to being able to access the Internet.

Goal 2 is to achieve universal primary education. Especially in rural areas, access to primary education is still a challenge in many developing countries. Technologies which support learning can have a positive impact. Think of initiatives like the 100-dollar notebook that are meant to bring access to knowledge to the most remote villages and to children who have been so far excluded from the information society.

UN Photo/Kibae Park

Population growth and the struggle for scarce resources - People queuing for water in Bangladesh

UN Photo/Olivier Chassot

Can ICT help poor countries in their economic development? Computers donated by the African Union and the United Nations in Darfur

Goal 7 is to ensure environmental sustainability. Although ICT is to a certain extent part of the problem through the use of energy and natural resources, like, for example, rare earths, ICT could also become an important part of the solution. ICT can help reduce energy consumption in households through smart metering, it can make power grids more effective, and it can reduce transport and CO_2 consumption by improving logistics and replacing business travel with web conferencing.

Goal 8, finally, is to develop a global partnership for development. The Internet has been one of the major drivers for the globalised economy. Internet-driven globalisation offers developing countries more opportunities to become part of global marketplaces and cooperate with partners from all over the world. Economic relationships between actors from developed and from developing countries may not always be equal. However, the rise of the BRIC countries Brazil, Russia, India, and China and the emergence of industry champions from these countries indicates that global economic relations could evolve towards more equal global partnerships.

In order to reap the benefits of ICT for supporting the Millennium Goals, more people need access to ICT services, and particularly the Internet. At the The World Summit on the Information Society governments agreed on ten targets, the Geneva Plan of Action, to be achieved by 2015. These targets include givingvillages universities, schools, hospitals, and public institutions access to information and communication technologies and to ensure that more than half the world's inhabitants have access to ICTs within their reach.

Conclusion

In 35 years, there will be nine billion people living on this planet. This is a huge challenge, but offers also opportunities. The challenge is to enable all of them to lead a life in dignity with a humane standard of living. Giving people access to ICTs could help in making this vision can become real.

Further information:
- UN world population statistics
  http://www.un.org/esa/population
- Millennium Goals
  http://www.un.org/millenniumgoals
- Worldometer population clock
  http://www.worldometers.info/world-population/