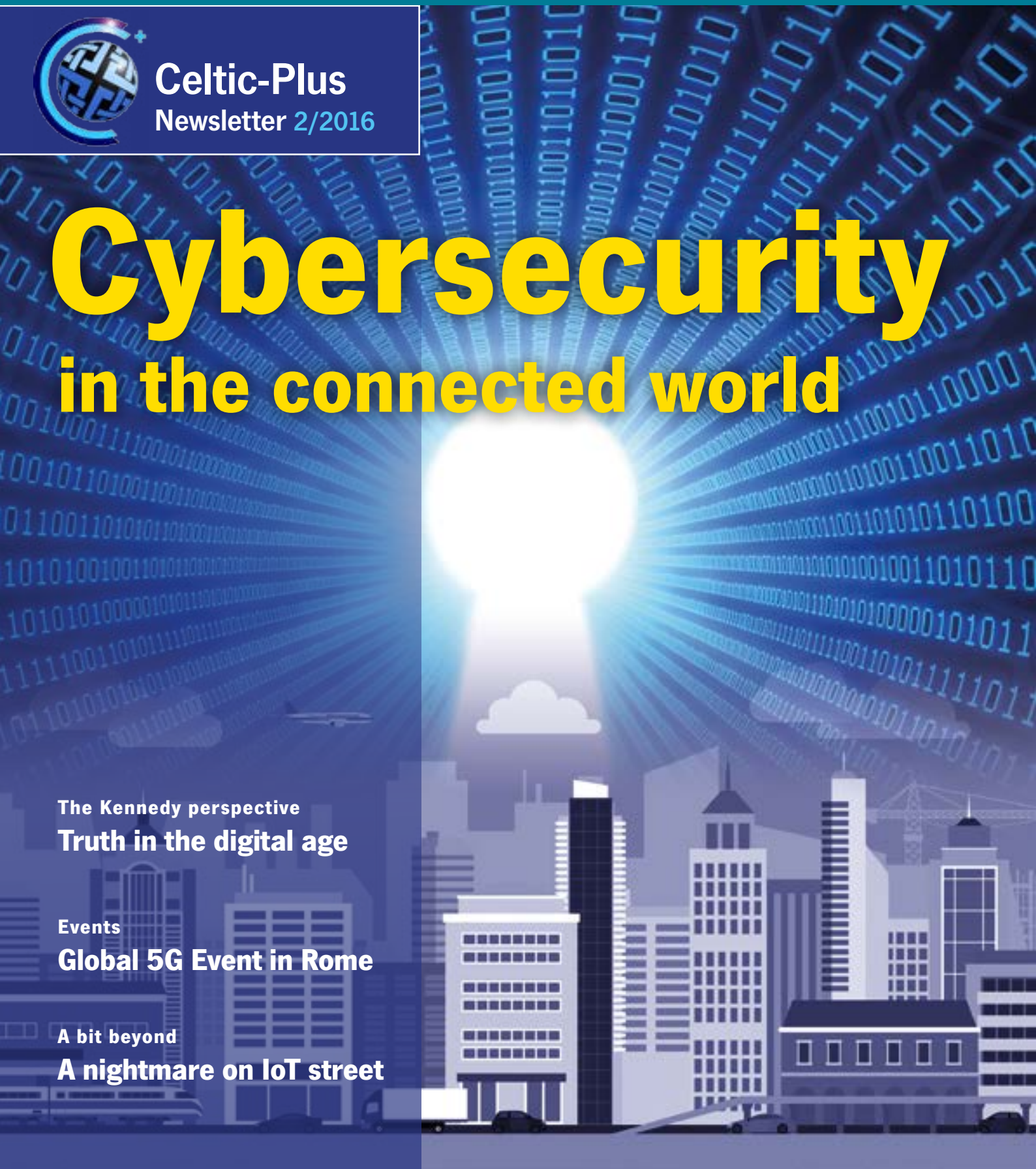
Winter 2016

EURESCOM message

The magazine for telecom insiders

Celtic-Plus
Newsletter 2/2016

Cybersecurity
in the connected world



The Kennedy perspective
Truth in the digital age

Events
Global 5G Event in Rome

A bit beyond
A nightmare on IoT street

Celtic-Plus Event 2017

Co-located with EUREKA Innovation Week 2017

Barcelona, Spain, 18 – 19 May 2017

The Celtic-Plus Event 2017 will be held on 18–19 May 2017 in Barcelona, Spain, co-located with the EUREKA Innovation Week 2017, which is organised and hosted by the Spanish EUREKA Chairmanship.

Networking with proposers and experts

The event will include a session on innovative project ideas for experts from the ICT community to discuss emerging R&D needs and proposals for related collaborative projects. This is an extraordinary opportunity for participants to present their companies and expertise, to offer project ideas for collaboration and to find partners.

Exhibition and demos

Results of about 15 commercially important Celtic-Plus projects will be presented at the related exhibition. The prototypes evolving from these projects will allow the audience to experience in an interactive and playful way the technological progress made in those projects.

Meeting funding representatives from national governments

Experts and representatives from national governments will explain their research agendas and the opportunities for public funding.

Celtic-Plus Award

Every year Celtic-Plus selects the three best rated Celtic-Plus projects for the Celtic Excellence Awards. At the event the winners will be announced and celebrated.

Further information:
https://www.celticplus.eu/latest-event/

Join the Industry-Driven Research Programme for a Smart Connected World

Celtic-Plus Call for Project Proposals – Deadline: 7 April 2017

Do not miss the opportunity to participate in Celtic-Plus, the industry-driven European ICT and telecommunications research programme under the umbrella of EUREKA. Submission deadline for the next call for project proposals is 7 April 2017.

Celtic-Plus projects are collaborative private-public partnership R&D projects. All EUREKA member countries and associated countries can financially support them. More information on public funding and national contacts per country can be found on the Celtic-Plus Public Authorities Website. Please talk to your national contact early in the process.

Easy proposal process

Preparing and submitting a Celtic-Plus project proposal is easy. Just register on the Celtic-Plus online proposal tool, fill in the Web forms, and upload your proposal in pdf format. Access to the proposal tool and to a proposal template is available via our Call Information page at https://www.celticplus.eu/call-information

Benefits of participating in Celtic-Plus

- You are free to define your project proposal according to your own research interests and priorities.
- Your proposals are not bound by any call texts, as long as it is within the ICT/telecommunications area.
- Celtic-Plus projects are close to the market and have a track record of exploiting their results soon after the end of the project.
- High-quality proposals have an excellent chance of receiving funding, with an average success rate of 60–70 %.
- The results of the evaluation will already be known in May 2017.

If you have any questions or need help, do not hesitate to contact us; we are pleased to help you.

Contact:

Celtic-Plus Office
office@celticplus.eu

Peter Herrmann
herrmann@celticplus.eu

Celtic-Plus
Smart Connected World

www.celticplus.eu

Dear readers,

We live in a world which is increasingly connected. That is a blessing and a curse. Making the transition from connected computers to connected things offers unprecedented opportunities. At the same time, it makes us more dependent on the flawless functioning of ICT and more prone to the risks of cyberattacks. According to the ITRC Data Breach Report 2015, more than 169 million personal records were exposed through data breaches in 2015, including personal health records.

In the emerging Internet of Things, more cyberattacks with a higher potential damage are to be expected. In 2016, we already got a taste of cyber threats to come. At the time of writing, at the end of November 2016, Germany was shook by a massive cyberattack. Almost a million routers of Deutsche Telekom customers were disrupted. The attack seems to have aimed at hijacking the router devices for launching a much bigger Internet attack.

Thus, improving cybersecurity has become a major societal challenge. Regulatory pressure on network operators, service providers, and manufacturers will increase to provide security solutions that make communication infrastructures more resilient against cyberattacks.

In this issue of Eurescom message, we present a selection of first-hand insights on European cybersecurity research. Our cover theme includes contributions by researchers working on different types of cybersecurity challenges.

In the first article of the cover theme, Adam Kapovits, project manager at Eurescom, provides an overview on cybersecurity challenges. The next article presents results from FP7 project RERUM for increasing security and privacy in the Internet of Things. This is followed by an interview on the status and future development of cybersecurity in Europe and worldwide with Dr. Steve Purser from ENISA. The next article presents solutions by 5G PPP project SELFNET for the self-protection of networks against botnet attacks. Concluding the cover theme, we present an article on the new Celtic-Plus project SENDATE-PLANETS, which will develop solutions for increasing the security of distributed datacenters.

This edition of Eurescom message also includes a variety of further articles on different, ICT-related topics. See, for example, the new opinion article by Eurescom director David Kennedy on trust in the digital age in his column "The Kennedy Perspective". See also our events section, which contains a report on the 5G Global Event in Rome. Finally, in the latest "A bit beyond" article you can learn about things to know about the Internet of Things.

My editorial colleagues and I hope you will find value in this edition of Eurescom message, and we would appreciate your comments on the current issue as well as suggestions for future issues.

Milon Gupta
Editor-in-chief

EVENTS CALENDAR

5 – 8 January 2017
CES Conference 2017
Las Vegas, US
https://www.ces.tech

27 February – 2 March 2017
Mobile World Congress – MWC 2017
Barcelona, Spain
http://www.mobileworldcongress.com

7 – 9 March 2017
20th ICIN conference – Innovations in Cloud, Internet and Networks
Paris, France
http://www.icin-conference.org

18 – 19 Mai 2017
Celtic-Plus Event 2017
Barcelona, Spain
https://www.celticplus.eu/

21 – 25 May 2017
IEEE International Conference on Communications ICC 2017
Paris, France
http://icc2017.ieee-icc.org/

12 – 15 June 2017
European Conference on Networks and Communications – EuCNC 2017
Oulu, Finland
http://www.eucnc.e https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA5-4759ENN.pdf u/

SNAPSHOT

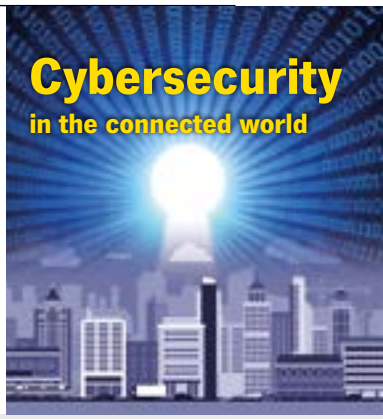
Robot solves Rubik's Cube in record time

A robot named "Sub1 Reloaded" solved a scrambled Rubik's Cube at a trade show in Germany in the record time of just 0.637 seconds. The fastest human needs at least 4.9 seconds to solve the puzzle. "Sub1 Reloaded" pulled off the feat with the help of microchips from Infineon and the microcontroller AURIX™.

Further information is available on the Infineon website at http://www.infineon.com/cms/en/about-infineon/press/press-releases/2016/INFXX201611-014.html

Photo: Infineon

Contents



Celtic-Plus Newsletter

Imprint

Eurescom message, winter issue 2016
ISSN 1618-5196 (print edition)
ISSN 1618-520X (Internet edition)

Editors: Milon Gupta (editor-in-chief), 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 message · Wieblinger Weg 19/4 · 69123 Heidelberg, Germany
Phone: + 49 6221 989-0 · Fax: + 49 6221 989-209 · E-mail: message@eurescom.de

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

Truth in the digital age

David Kennedy
Eurescom
kennedy@eurescom.eu

Most of us are really fed up with the American election and the UK referendum, not because we don't take politics seriously, but because these votes have brought us into what the Oxford Dictionary now refers to as the "post-truth politics". Post Truth is defined as relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.

"Falsehood flies"

It is not a new problem, as Jonathan Swift wrote on this topic in "The Examiner" in 1710: "Besides, as the vilest Writer has his Readers, so the greatest Liar has his Believers; and it often happens, that if a Lie be believ'd only for an Hour, it has done its Work, and there is no farther occasion for it. Falsehood flies, and the Truth comes limping after it; so that when Men come to be undeceiv'd, it is too late; the Jest is over, and the Tale has had its Effect..."

Our new dependence on messaging, always-on communications and social networks has left us even more vulnerable than ever to being deceived by fast moving unsubstantiated "news".

Jonathan Swift, early explorer of falsehood and truth

The city of Veles in Macedonia, source of false news

Facebook are particularly guilty here in that, for fear of being accused as biased, they abdicated using intelligent people as filters to stop the propagation of untruths and left it to "intelligent" programmes to trend "news" based solely on popularity.

News from Veles

The end result of this is that we have had a rapid development from a number of reasonable satire sites to a large number of less reasonable satire sites that promote false news, and finally to a huge number of clickbait sites. These clickbait sites promote any dramatic headline – usually totally false – in order to get people to visit their sites. For example, more than 140 US election related sites pushing bad news have been traced by BuzzFeed to a single town in Macedonia: Veles [1]. BuzzFeed reports that the student site owners don't care about politics or the effect their false news is having, because they are making money from advertising. The fact is that there is a clear economic incentive for producing false information supported by our use of social media. Of course, the question still remains, if we can trust Buzzfeed's article, as it is cyberspace too.

Google has realised that this problem exists and has announced that it will ban websites that deceptively present fake news as real. However, to do this it has to identify them and make a judgement. It is not always easy to distinguish satire from lies, and Google has been tricked into promoting fake news based on trends enough times for it to see the new policy of banning false news was needed.

Conclusion

So we have several problems here – the problem of the propagated lies influencing the outcome of important decisions, the problem of policing the information space to stop lies, and the problem of people being paid to mislead us.

What can we do? Can the ICT community come up with a truth filter for our communications? Should we? Whose duty is it? Maybe Artificial Intelligence, regarded by some people as a risk to mankind, could turn out to be the necessary tool to protect us from ourselves and preserve the truth.

References

[1] https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.cdqVX6Oo5#.nx83pXLgv

Cybersecurity challenges – An overview

Adam Kapovits
Eurescom
kapovits@eurescom.eu

Cybersecurity is becoming a cornerstone element of the trust needed to ensure the proper functioning of our digital society. Integrity of the communication infrastructure, the many smart devices connected, and the data and information generated and collected are critical, and need to be protected. At the same time there is an increase of cyber-attacks that exploit weaknesses of ICT systems for financial, political or military gains.

Cybersecurity is recognised as a global challenge, not only by experts, but also by businesses and politicians. In 2014, security firm McAfee valued the annual cost of cybercrime to the global economy at more than 400 billion US dollar (Net Losses: Estimating the Global Cost of Cybercrime, McAfee report, June 2014).

European cybersecurity activities

On the political level, the European Commission considers cybersecurity as a top priority essential for Europe's economic prosperity and competitiveness. This fact is clearly reflected in the release of the European cybersecurity strategy in 2013. Furthermore, cybersecurity is a key foundational element to ensure trust in digital infrastructures, necessary to deliver on the goal of the Digital Single Market set out by the European Commission.

The potentially high gains through exploits by cybercrime provide sufficient incentives with the effect that threats are growing dynamically in numbers and broadening in scope. The evolution of technology provides additional levers, as more capabilities induce more vulnerability. To counter this, numerous sector-specific, regional, national, multi-national and global initiatives have been launched. They include the recently started European contractual Public Private Partnership on Cybersecurity and the establishment of the European Cybersecurity Organisation (ECSO). To achieve their ultimate goal and deliver a safer society with greater trust, they need to collaborate and align their activities.

Let us briefly survey the various technology domains particularly concerned by cybersecurity.

The CIA triad

What exactly is cybersecurity? ISO/IEC JTC1 defines cybersecurity as the preservation of confidentiality, integrity and availability of information in Cyberspace. It is widely recognised that cybersecurity is based on this CIA triad of confidentiality, integrity and availability (see figure). In this context, 'confidentiality' means that data is accessible and available only to intended recipients. Technical solutions to preserve confidentiality include first and foremost encryption.

'Integrity' means that the system and the data in it have not been improperly altered or changed without authorization. Integrity requires guarantees yielding to confidence both in the system and data. Mechanisms to assure data integrity include digital signatures.

Availability means being able to use the system as anticipated and obtain and access data as and when required without constraints. High levels of availability assume a certain resilience of the system. Resilience means that the system can endure a broad range of technical conditions including even cyber-attacks and remain operational without critically failing.

Let us see and discuss cybersecurity in terms of the three main technical domains concerned, hardware, software and communication.

Hardware aspects of cybersecurity

A broad range of solutions rely on using hardware-based security enforcement, smart cards and embedded micro-electronic solutions and chips for authentication, authorisation and access control, as well as to support the task of encryption.

Concerning the Internet of Things (IoT) domain, sensors and embedded devices are becoming more and more capable, and are growing explosively in numbers in all areas of life. The IoT edge formed by those devices represents the primary attack surface due to the resource constraints of the devices and the associated difficulty to adequately protect them. This is exacerbated by their physical exposure, being deployed in uncontrolled, or difficult to control environments in most cases.

This situation is expected to prevail even in the long term, as the exposure and resource constrained nature are intrinsic characteristics of the edge. Admittedly, technology advancement is expected to make edge devices more resourceful and less constrained over time. However, this will not change their position as remaining the weakest point in the IoT – the same level of sophistication and protection that is available in more controlled environments and closer to the core of the system will not become feasible. So the edge is expected to remain the main battlefield with a continued arms race between defence and at-

Cybersecurity and the CIA triad of confidentiality, integrity and availability

tack, with the defence being in a disadvantaged position.

Cybersecurity in communication networks

Cybersecurity in communication networks essentially means the protection of data against eavesdropping while they are in transit from one system to another. Confidentiality is assured using cryptographic measures, and the integrity of the information through the use of appropriate signature mechanisms. It also guarantees for delivering it to its intended recipients, and only to those, in a timely manner. This means that in an IoT context user data and, measurement data supplied by the distributed sensors are available as and when users and applications demand them; the data remain confidential and their integrity is preserved. In the reverse direction, the integrity of commands as well as software and firmware updates sent to sensors and actuators are preserved.

Software aspects of cybersecurity

Over the years software has been evolving to become the central element of all ICT systems. The recent trend is that all systems are somehow software defined and driven. This ranges from software defined radio, software defined networking up to the complete infrastructure that is being virtualised, meaning software defined. Advances in software engineering accept today that there are two main causes leading to security problems.

The first problem is non-conformance or a failure to satisfy a given requirement. In most cases non-conformance is easy to deal with, using modern tools for verification and validation. The second problem is the omission or an error in the requirements. Unfortunately security problems induced by missing, incomplete, or inappropriate requirements are more difficult to identify. This typically originates in a failure of the requirements engineering process phase of the software development. To respond to this problem, software security assurance must at least ensure that security requirements have been established and a security evaluation has been performed. This is an important statement, which directly implies that software security assurance must be an integral part of software development.

However, a near-term problem is that cyber physical systems are complex systems, potentially involving multi-disciplinary aspects, and the approach to protect them with conventional measures may not be adequate any longer. Considering complex systems theory, it is important to understand how the different parts of a system interact with each other, the environment and the human, resulting in a collective behaviour. As a consequence we need to develop new strategies for testing and validation of complex cybersecurity systems that embrace holistically more than just ICT related disciplines.

Good design practice – security by design

An essential design practice to improve on the current situation – and not only regarding software aspects – is that security aspects and requirements must be considered upfront. Unfortunately, even recently, the competitive pressure on technology providers acts in such a way that providers rather focus on bringing solutions with new features on the market that differentiate them from other providers and give them an advantage over them, and tend to relegate security concerns to secondary importance. There is a major issue with this practice. Security is not something that can be just retrofitted onto a solution. In many cases it might be simply impossible, or prove to be prohibitively expensive. There is a consensus by now, that security is something that should be considered in the design phase. A good example for this security by design approach is the EU FP7 project RERUM: Reliable, resilient and secure IoT for smart city applications that devised an IoT architecture for smart city applications.

Outlook

It is reasonable to expect in the coming period of continued rapid evolution of technology that there will be an arms race between defence and attack. Research, business and policy making need a concerted effort to stay on top of this struggle and deliver on the promising vision of digital society very much rooted in cybersecurity.

Further information:
EC web pages on cybersecurity – https://ec.europa.eu/digital-single-market/en/cybersecurity
ECSO website – http://www.ecs-org.eu
EU FP7 RERUM project – https://www.ict-rerum.eu

Security and privacy in the Internet of Things

Results from the RERUM project

Elias Tragos
FORTH-ICS
etragos@ics.forth.gr

The Internet of Things (IoT) is presented as a promising technology for simplifying the development of smart applications in areas such as cities, industry, buildings, and agriculture. Although many IoT devices and applications are on the market, only a small percentage of them are designed with security and privacy considerations. Most of them adopt only a bare minimum set of respective functionalities. The dilemma that developers are facing is the trade-off between security, privacy and performance. Thus, the question that arises is: are security and privacy in IoT obstacles or necessities?

IoT product landscape regarding security and privacy

IoT applications are all around us. Both large and small/medium enterprises have acknowledged the potential revenues in IoT and are trying to get their own share in the huge IoT market, which is currently in its infancy. There is a big misunderstanding in the market: every product that has a chip and a radio interface embedded and is capable of connecting to the Internet and send data to a remote server is promoted as an "IoT device". Most of these products do not support key IoT characteristics, such as interoperability, heterogeneity, virtualization and intelligence. They basically support the client-server pattern and are able to "talk" only to remote servers.

Another key drawback of most existing IoT products is the lack of embedded security and privacy functionalities. The widely used phrase "a system is only as secure as the weakest link" applies also to IoT systems, where the "weakest links" are the end devices, due to their technical limitations. IoT devices are usually constrained devices that have limited resources in terms of CPU, memory, storage, and battery. For example, a recent IoT product, which is considered state of the art in its target application area, developed within the RERUM project is the Zolertia RE-Mote, which has a 32MHz CPU, 32KB of RAM and 512KB of flash storage. It is reasonable to assume that in such products it is not easy or even possible to embed strong security and privacy functionalities, without severely impacting performance. This was also proven by the RERUM project (Reliable, resilient and secure IoT for smart city applications) [1], where the trade-offs between security functionality and performance of the IoT devices were presented. Therefore many developers assume that building a product that performs well can be promoted better in the market than a more secure product with lower performance. For this reason they neglect security.

A recent report by HP [2] analysed the security of existing IoT devices and the results seem quite alarming. Most devices collect and transmit personal information, use unencrypted communication channels or don't require strong passwords. Such examples are becoming daily news. There are reports about smart fridges being hacked to send spam mails, smart lightbulbs having vulnerabilities that can allow attackers to gain access to the home network, smart plugs that can be controlled by anyone that knows their MAC address, and smart cars with weak pre-shared keys that can be easily cracked allowing malicious users to control the car.

The privacy-related incidents are similarly worrying. Many IoT products send unnecessary data to servers on the Internet without notifying the customers. For example the Nest thermostat has been leaking information such as home location and zip code without any encryption. Security cameras transmit video over unencrypted FTP. Fitness trackers store all data unencrypted or don't use any encryption when transmitting data. Finally, there is a smart vibrator which sends intimate usage data to the manufacturer and which is controlled by an app without security (see also the "A bit beyond" article in this use).

Even large companies don't pay the necessary attention to the security of their devices. The impact of using unsecure devices can be tremendous for the end users: data loss, data corruption, denial of service, denial of access, identity spoofing, device compromise, lack of accountability, and leakage of personal data to unauthorised third parties. These can become barriers for the adoption of IoT products and applications by the citizens, as they will consider IoT an untrustworthy technology.

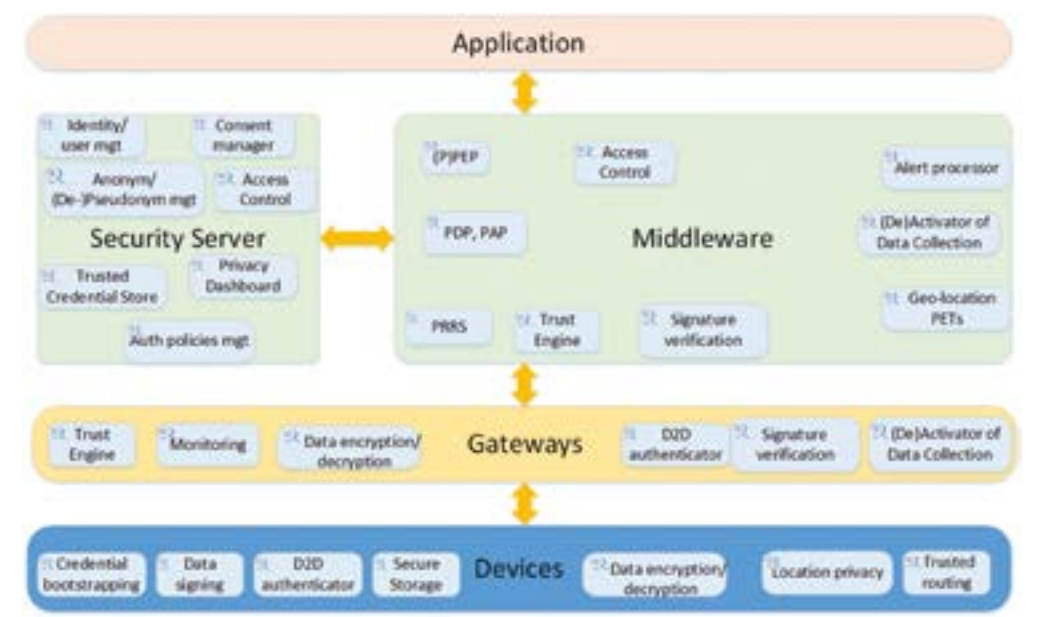
RERUM vision for secure IoT

To improve the trustworthiness of IoT, RERUM proposed a holistic and cross-layer IoT architectural framework, based on the concept of "security and privacy by design". The framework includes functionalities for securing and protecting data across their entire lifecycle from data generation up to their use in the applications (see Fig. 1 and [3] for more details). The functionalities are split into three groups for (i) security, (ii) privacy and (iii) trust and are embedded in all system components; end devices, gateways, middleware and applications. This is required to secure the whole data lifecycle and avoid leaving a system component unprotected [3].

RERUM from its inception had the focus on designing and developing lightweight security functionalities that could be executed in constrained environments without severely affecting performance. The theoretical analysis and the experimental evaluation of the techniques developed by RERUM showed that embedded security, if properly designed, is not a hurdle for performance.

RERUM proposed a number of required mechanisms that should be applied even on constrained devices, such as lightweight encryption either on the transport layer or on the application layer using the Compressive Sensing (CS) theory. This technique uses information regarding the sparsity of the signal that is being measured in order to identify the percentage of compression that can be achieved without losing significant information and achieves simultaneously compression and encryption [4].

Data integrity is quite important in IoT, because manipulation of measurement values can affect system decisions. For example, if a malicious intermediate node alters the values reported by a temperature sensor, the home automation system will continue to have the air-conditioning system working in the highest mode, increasing the electricity consumption of the household. To avoid such events and protect the integrity of the data digital signatures on the devices should be used so that no unauthorised intermediate can alter the data without being detected. Signatures can also be used for privacy protection in the cases when authorized intermediates alter parts of the data concealing potentially sensitive or unneeded information, yet allowing the verification of the signature in the middleware or the application.



Basic RERUM functionalities for security, privacy and trust

Moreover, data minimization techniques should be applied either on the devices or on the gateways to support privacy protection. Data minimization means transmitting the required data only, and no additional unneeded data that can be correlated with other data to obtain unauthorized knowledge. In the RERUM solution no identifiers (i.e. addresses, names, locations) are transmitted. Thus, the applications cannot link the data to specific devices or users. Additionally, the applications are getting only the type and format of the data they require. It means that if an application requires the average temperature in an area, it will get only this average value and not the raw data from the sensors in order to calculate the average at a later stage.

Moreover, RERUM proposes to include privacy-enhancing techniques in the whole system and not only on the devices. Anonymization and pseudonymisation techniques must be used when dealing with user data, together with access control derived from user-defined access and privacy policies. RERUM allows the user to have full control over its data and is able to identify who accesses or wants to access the data and for what purpose. The user can grant or revoke consent to such data collection. The RERUM middleware provides functionality for activation and de-activation of data collection from devices, translating the corresponding commands from the users and forwarding these commands to the gateways and devices.

Trustworthiness of IoT

IoT trustworthiness has to be taken seriously in order to widen the adoption of IoT technologies and products by citizens, end users and municipalities. The notion of trust incorporates security, privacy, reliability and increased availability. RERUM proposed functionalities that can work for increasing the trust in IoT, by analysing and assessing the reliability of the data provided to the applications and by assigning trust ratings to services, data streams and devices. An application can query the reputation manager and request data from services that have a specific reputation. The system administrator can be alarmed when the reputation of devices or services drops below a threshold. The latter case is important during incidents of system attack or data manipulation attempts, but also when devices are malfunctioning or indicate exceptional events. For example, a fire can raise suddenly the temperature in a specific area. Trust assessment of data, services and devices can be performed by various system components, for example by the gateway to identify local anomalies or by the middleware to obtain a global view of the situation.

Most of the described functionalities have been implemented and tested in real world trials in two municipal environments, Heraklion in Greece and Tarragona in Spain. The results of the evaluation in the trials showed that even in real environments security and privacy components can work well without affecting the performance of the system, while decreasing the possibility of data being stolen or manipulated by external parties.

Conclusion

IoT is all around us, and almost every day new products are introduced to the market. Companies are rushing to sell products and take a share of the IoT market, focusing on promoting the innovation of the product ideas. Most of these products lack basic security functionalities, which make them vulnerable even to simple attacks, such as eavesdropping. Hackers and attackers have focused recently on IoT products, because they see them as a new challenge that goes beyond the standard PC hacking, and because they affect the physical world. A hacker has more fun playing with the blinds or the lights of his neighbour than putting a virus on his computer. However, a more serious attacker might also be able to hack the front door or the windows and enter the house or harm the user by shutting the door when he tries to go through.

The RERUM project has released a basic architectural framework and a set of security, privacy and trust functionalities that help making IoT products and applications much safer and trustworthy. RERUM has proved that embedding a minimum set of functionalities in constrained IoT devices is not an unrealistic task and can be done without significantly affecting performance or battery life of the products. Security and privacy in IoT do not have to be considered as a hurdle, but can be used as tools to avoid making the IoT world an open field for cyberattacks.

References

[1] V. Angelakis, et. al. Analysis and Evaluation of system performance and scalability. RERUM Deliverable D4.3, April 2016.
[2] Internet of Things research study. Hewlett Packard Enterprise 2015 report, available online at: www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf
[3] RERUM website – https://ict-rerum.eu
[4] E. Tragos, et. al. Final System Architecture, RERUM Deliverable D2.5, August 2015.
[5] Fragkiadakis, Alexandros, Pavlos Charalampidis, and Elias Tragos. "Adaptive compressive sensing for energy efficient smart objects in IoT applications." Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on. IEEE, 2014.

We need a strong European cybersecurity industry

Interview on cybersecurity with Steve Purser from ENISA

Threats to the security of digital data and networks have been dramatically increasing over the past years. The prospects for the coming years appear even more challenging. Eurescom message editor-in-chief Milon Gupta asked Dr. Steve Purser from ENISA, the European Network and Information Security Agency, about his insights on the status and future development of cybersecurity in Europe and worldwide. Dr. Purser is head of the core operations department at ENISA (www.enisa.europa.eu).

Which major cybersecurity threats is Europe facing today and in the near future?

Steve Purser: Ongoing threat analysis has shown that threats like malware, phishing, ransomware, insider threat, botnets and denial of service attacks can cause significant impact to European organisations and companies. On the other hand, the market for zero-day vulnerabilities flourishes: in 2015 we have seen an increase of zero-day vulnerabilities of more than 100 %. The assessed cybersecurity threats together with existing zero-day vulnerabilities pose a severe risk in cyberspace.

In the near future, the assessed cyber-threats may find fertile ground in emerging technological deployments in the areas of Internet of Things, Smart Environments, Mobile Environments, E-Health and many more. Hence, while cybersecurity threats develop further, their impact depends on the vulnerabilities and protection level implemented in various technology platforms.

What is the EU doing to mitigate the growing cybersecurity risks?

Steve Purser: Europe has a range of ongoing activities to mitigate cybersecurity risks. The EU cybersecurity strategy, the Network and Information security Directive (NISD), the newly formed public-private partnership on cybersecurity (cPPP) and the General Data Protection Regulation (GDPR) are illustrative examples. These approaches include many cybersecurity provisions such as capability building, training, public private partnerships, coordination, information sharing, awareness raising, policy making, recommendations, development and dissemination of good practices and knowledge, standardisation, and education. As EU initiatives, the general approach is to include all relevant stakeholders such as governments, vendors, consumers, law enforcement and various end-user groups.

Dr. Steve Purser, head of the core operations department at ENISA

Within the context of the NIS Directive, ENISA will work with the Commission and the Member States to define baseline security requirements for operators of essential services in order to support harmonization across Europe. The main objective of these efforts is to disseminate available baseline, common sense cybersecurity knowledge, while at the same time strengthening engagement in maintaining available security levels.

Finally, the Commission continues to foster collaboration with stakeholders by using existing platforms and fostering research and development (R&D) in the area of cybersecurity. ENISA fully supports this approach and has also developed a number of such platforms to support its own contribution. Examples of the latter include the ENISA Industrial Event, The Annual Privacy Forum (APF) and, in collaboration with the Commission, the EU Cyber Security Month (ECSM)

In autumn 2016, ENISA conducted another cybersecurity exercise. What was the purpose?

Steve Purser: The objectives of Cyber Europe 2016 were to test both national and EU-level cooperation in the event of a cyber crisis and to train the capabilities of participants. Through the exercises, the EU is enhancing its preparedness to tackle current and future cybersecurity challenges.

Concretely speaking, the exercise provided numerous opportunities to improve cybersecurity technical skills, but also to improve business continuity processes and test organisational, national and European level cooperation processes. As such, cyber exercises are an essential part of the EU cyber crisis cooperation lifecycle.

Ultimately, exercises such as Cyber Europe 2016 enable the European cybersecurity community to further build its capacity in identifying and tackling large-scale threats, to better understand cross-border incident contagion and to reinforce cooperation amongst public and private entities, hereby reinforcing the overall level of cybersecurity in the European Union. In particular, exercises are key in helping to increase the preparedness of the EU critical infrastructures.

How well prepared are companies, government agencies and citizens to deal with cyber threats?

Steve Purser: Today, most countries have a national or governmental computer security incident response team and many have a cybersecurity agency. Cybersecurity strategies have been drafted in most Member States, prevention and crisis plans written and critical infrastructure operators designated. As a result, cybersecurity is often one of the priorities of the boards of such operators. Nevertheless, much remains to be done, notably for SMEs.

In order to support companies, governments and citizens in dealing with cyber threats, the EU needs to develop a strong European cybersecurity industry. Whilst there are many small companies offering innovative solutions in the area of cybersecurity, there are a number of barriers preventing such companies to grow and compete on a global level. Through its Industry Event and other contacts with industry in the context of the annual work programme, ENISA is helping to raise awareness on the supply and demand for security products and services within the EU, thereby helping SMEs specialising in cybersecurity to compete more effectively in the global marketplace. ENISA also actively supports PPP initiatives of the Member States and the Commission including the recently launched cPPP for cybersecurity.

One of the biggest challenges facing the EU in the area of cybersecurity is adapting to the increasingly rapid availability and deployment of new technologies. This is typified by the so-called Internet of Things, which is a collective name for a global network of distributed devices or 'objects' that can communicate with each other over the Internet. The challenge for the EU is to achieve a sensible balance between economic considerations and security considerations that will allow EU companies and citizens to benefit from the opportunities afforded by this model whilst still retaining an appropriate level of security.

What should Member States do to better protect critical infrastructures against cyber incidents?

Steve Purser: ENISA invites the Member States to adopt a number of recommendations in order to improve their national cybersecurity capabilities.

We recommend that they identify and define the roles of the entities responsible for cybersecurity. A collaboration platform should be foreseen in case more than one authority is designated. Furthermore, they should develop a national framework and align critical infrastructure protection governance with their existing national cybersecurity strategy.

Member States should also perform national risk assessment exercises. Such risk assessment approaches are highly recommended and planned to be used by some Member States, as well as business continuity measures implemented looking for the maximum availability of the service and infrastructure associated.

We also recommend to establish a national forum on cybersecurity with maximum representation of the public and private stakeholders. A successful cybersecurity programme requires proper co-operation between public and private stakeholders. Identifying and engaging stakeholders are crucial steps for the success of the programme.

In addition, it is crucial to establish trusted national information-sharing mechanisms for cybersecurity. Asset owners could potentially share with public authorities their input on mitigating emerging risks, threats, and vulnerabilities while public stakeholders could provide on a 'need to know basis' information on aspects related to the status of critical infrastructures' cybersecurity.

We consider it also important to establish a national incident response capability. Due to the increased level of interconnectivity among its devices, critical infrastructures are vulnerable to a greater number of cyber-attacks. A computer emergency response capability in order to counter these attacks makes sense.

On a user level, Member States should undertake awareness activities on smart grid privacy and security such as awareness raising campaigns, workshops, conferences, and happenings.

Finally, Member States should join international forums and workgroups on cybersecurity. In this fast-changing environment, it is very important to stay up to date of the success and failure stories behind implementation projects, technologies, frameworks, approaches or regulations. Sharing information and experiences with other international stakeholders in these international fora, workgroups and initiatives proves beneficial. Tools such as the NISD Cooperation Group and the CSIRT network are extremely useful for this purpose.

In which way is the growing level of interconnection via the Internet of Things and machine-to-machine communication opening the door for a new level of exposure to cybersecurity risks?

Steve Purser: The expected growth of the Internet of Things will drastically increase the attack surface. Today, there are about 10 billion connected devices; by 2020 it will be three times more. Defending such a network of equipment will pose new challenges, which will require a paradigm shift from how we approach cybersecurity today.

Fast time-to-market, cheap equipment, limited computing power and networking capabilities all pose significant problems to the implementation of security in the design of these devices, as well as to their maintenance. As a result, billions of devices could remain unprotected to viruses, denial of service attacks, man-in-the-middle attacks, interceptions, and more. Also, due to their very nature, connected devices in the Internet of Things will be much more exposed, and hence much more prone to physical attacks than traditional IT systems. Their penetration in our private life will bring privacy breaches and ransom attacks to a whole new level, while their increasing use in industrial control systems will also open the door to more cyber-physical attack scenarios.

What is your vision for cybersecurity in Europe by the year 2021?

Steve Purser: Cybersecurity is the key to preserve the values we cherish in Europe in the digital age. Such values do not change rapidly, but the technological landscape in which they need to be preserved does. Our vision to protect these values by 2021 is based on the following points:

We need mature capabilities deployed in a harmonized manner across European Member States and institutions, as well as enhanced co-operation between Member States; the NIS Directive is an unprecedented step in this direction.

We need a strong European cybersecurity industry. This involves fostering a stronger ICT and IT security industry to compete successfully in global markets and ensure better control over our digital activities. In addition, it is critical to ensure the security of the supply chain for the technologies manufactured outside Europe, which are essential to our cyberspace.

With the increasing digitization of private life and the forecasted exponential growth of the Internet of Things, European citizens will be much more exposed to cyber-attacks than in the past, and thus need to be protected and more aware of their cyber environment. This is why, last but not least, we need to bring cybersecurity down to the citizen level.

Celtic-Plus Newsletter 2/2016

More secure data centres in Europe – SENDATE kick-off event

SIGMONA – Software Defined Mobile Networks

How Sweden manages the Celtic-Plus project process

Editorial

Table of Contents

IMPRINT

Editor-in-chief:
Peter Herrmann
herrmann@celticplus.eu

Contact:
Celtic Office
c/o Eurescom GmbH
Wieblinger Weg 19/4
69123 Heidelberg, Germany
Tel: +49 6221 989 381
Fax: +49 6221 989 451
www.celticplus.eu

Dear readers,

Is there a framework for collaborative international research that is closer to the market's needs than the EUREKA Clusters and Celtic-Plus? I am convinced that the structure of Celtic-Plus, which is controlled by a core group that brings together the most important industry players in our technological field, is quite unique. Furthermore, the experts who are evaluating the incoming proposals and who are doing the review of the running or finishing projects are mostly from industry and have a clear view on the market's needs.

Together with the bottom-up approach that allows industry and their partners to bring in any R&D subject that might become the next hot topic, the Celtic-Plus framework ensures the focus on technologies that are needed for the market. This view is shared by many of our customers. One of them, the Swedish funding agency VINNOVA, explains their view on the bottom-up, simple and agile Celtic-Plus process in this newsletter.

In 2016, two new members have joined the Celtic-Plus Core Group: Netaş from Turkey and imec from Belgium. Netaş is a fast-growing Turkish ICT company with a strong focus on innovation, and imec is an important Belgian research laboratory that has obtained an observer status in the Celtic-Plus Core Group. Both organisations have already proven their dynamism and their value for Celtic-Plus in giving decisive help for the organisation of the Proposers Days in Istanbul and in Leuven. You can read about both events in an article in this issue.

Also the Celtic-Plus Management team changed in 2016. Jukka Salo retired from Nokia and from his role as Celtic-Plus Vice-Chairman. I would like to express my gratitude for the huge work that Jukka has contributed during all these years in his role as Celtic Vice-Chairman, and I wish him all the best for his new life phase in his house in Finland. The Core Group has decided to strengthen the management team. In addition to the Celtic-Plus Chairman Jacques Magen and the Vice-Chair Valerie Blavette from Orange, the Core Group appointed two new Celtic-Plus Vice-Chairs: Jari Lehmusvuori from Nokia and Riza Durucasugil from Netaş. We welcome both and we are glad having their support that will be very much appreciated. Both new Celtic-Plus Vice-Chairs will be introduced to you in a separate article.

One of this year's highlights for Celtic-Plus was the start of a new flagship project: On 17 October 2016, the Celtic-Plus flagship project SENDATE was officially launched at a high-level event in the centre of Berlin. Read more about the project and the event in this issue.

SENDATE was not the only new project: In 2016 12 new Celtic-Plus projects secured funding and could start their work. In the same period 9 new projects were labelled, 5 in the Spring Call and 4 in the Autumn Call. 11 labelled projects are still in the set-up phase – the big challenge is to get also these projects funded and running.

Finally, we present in this newsletter three very successful Celtic projects that finished their work in the last year: SIGMONA, SHARING and TILAS.

For 2017, the Celtic-Plus Core Group has already fixed three important dates: On 21 February, we will organize the next Proposers Day at the Telecommunication Innovation Laboratory of Deutsche Telekom in Berlin. A preliminary programme is available on the Celtic-Plus Website; the registration will open in December. The date of the Spring Call has been decided, it will be on 7 April 2017. The Call information is available on the Website, and I hope that we will receive many very innovative project proposals. Next year we will organize the Celtic-Plus Event in Barcelona on 18-19 Mai 2017. It will be collocated with the EUREKA Innovation Week that will be hosted under the Spanish EUREKA Chairmanship.

I would like to express a big thank you to our very dynamic community. More than 50 project pitches at this year's Proposers Days in Madrid, Stockholm, Istanbul, and Leuven are proof of the strong commitment. I hope that we will meet again next year in Berlin, Barcelona and other nice places all over Europe.

Peter Herrmann
Editor-in-chief

New Celtic-Plus Vice-Chairs: Riza Durucasugil and Jari Lehmusvuori

In the Celtic-Plus Core Group meeting on 22 November 2016, the Core Group members elected two new Celtic-Plus Vice-Chairs: Riza Durucasugil from Netaş and Jari Lehmusvuori from Nokia.

Riza Durucasugil
Director of Technology Solutions at Netaş

Riza Durucasugil is Innovation and R&D Strategies Director. Previously, Mr. Durucasugil worked in Netaş as Director of Technology Solutions, Software Design Team Senior Manager and Software-Development Manager and Software Designer. He is also the Steering Board Member of ARGEMİP R&D Center's Communication and Cooperation Platform, member of R&D committee of YASED International Investors Association and member of the R&D committee of TUSIAD, the Turkish Industry and Business Association. He graduated in Electronics and Communication Engineering and has a Bachelor of Science degree from Istanbul Technical University.

He has broad management experience in information and communication technologies, technical and business leadership qualifications with 20+ years of hands-on experience in developing strategies and businesses, planning multi-million dollars budget, leading large organizations and proven ability in the development of innovative, cost-effective and competitive business solutions to increase revenue and customer service offerings with establishing high-tech businesses and technology organizations.

Jari Lehmusvuori
Head of Department at Nokia Bell Labs

Jari Lehmusvuori is a Head of Department at Nokia Bell Labs, the research unit of Nokia, in Espoo, Finland. He is responsible for research and innovation on the future mobile networks architecture with a special focus on the core networks. The main focus is on the 5G mobile networks by applying the latest technologies such as network functions virtualization, software-defined networking and cloud computing. He has long-term experience in the area of mobile networks and systems through his engagement in the research and definition of 3G and 4G mobile systems.

He has been involved in several European research projects, including the role of project coordinator for the Celtic-Plus projects MEVICO and SIGMONA. He and the research team in Nokia Bell Labs are playing a role in the TAKE-5 research project of the 5G Test Network Finland, the Finnish national activity on 5G under the Tekes programme 5thGear.

More secure data centres in Europe

SENDATE kick-off event in Berlin

Peter Herrmann
Celtic-Plus Office
herrmann@celticplus.eu

From left to right: Tor Björn Minde (Head of Research Strategy, Ericsson), Jörg-Peter Elbers (Vice President Advanced Technology, ADVA), Sigurd Schuster (Head of Business Operation MN CTO, Nokia), Bernd Sommerkorn-Krombholz (Manager Optical Technology & Performance, Coriant). [Photo: © 2016 Steffen Gebert]

On 17 October 2016, Celtic-Plus flagship project SENDATE was officially launched at a high-level event in Berlin. The 80 project partners from Finland, France, Germany, and Sweden will develop solutions for more secure data centres in Europe.

The main goal of the three-year project coordinated by Nokia is to pave the way to a new type of network through delocalised and securely connected date centres. SENDATE will work on a solution to connect European data centres through enhanced transport networks and improved networking concepts that will results in reinforced overall security. The project will lead to better control of data flows and new security concepts on the internet.

Dr. Ulf Lange from the German Ministry of Education and Research, BMBF, underlined at the kick-off event that current trends towards Industry 4.0 and autonomous driving are good news for Europe and its industries, as these technologies generate a strong need for new types of network functionalities and data centres with low latency. This, he explained, creates new demand for network architecture and network performance, and it offers European companies a unique opportunity to market new communication technologies made in Europe.

Dr. Lange stressed that no country can do this alone. He said that only when Europe's public and private actors join forces and bring together the political and technological capacities to act on this global issue, Europe can be successful. This is why policy makers and industry from Finland, France, Sweden and Germany have invested 70 million euro to initiate this common undertaking. They consider the project a central pillar for enabling the safe, reliable, and stable communication networks of the future.

Mr Benjamin Gallezot, Deputy Director General at DGE, France, underlined the importance of SENDATE for France and Europe. The main objectives of SENDATE are perfectly in line with the actual goals of the industrial policy defined by the French Ministry of Economy and Finance in its programme "Nouvelle France Industrielle". Mr Gallezot is convinced that SENDATE will set standards for European industry. He stressed that the project is very important for the whole European telecoms industry.

Dr. Raine Hermans, Director of International Operations at TEKES, Finland, talked about open innovation. In Celtic-Plus open innovation is built in through a structure of sub-projects that allows to continuously align objectives and to have even competitors jointly contribute to these objectives. According to Mr Hermans, this can be the starting point for contributing to future application spaces.

From left to right: Dr. Ulf Lange (Head of Unit, Communication Technologies, IT-Security, BMBF), Dr. Raine Hermans (Director, International Operations, TEKES, Finland), Benjamin Gallezot (Deputy Director General, DGE, France), Jon Simonsson (Deputy Director General at Ministry of Enterprise and Innovation, VINNOVA, Sweden), Jacques Magen (Celtic-Plus Chairman). [Photo: © 2016 Steffen Gebert]

He shared his vision about a future without hospitals. He pointed out that if we do not have a really challenging vision for the future, we are just incrementally improving today's solutions. We need to start building entirely new systems and systemic innovation. Mr Hermans challenged the SENDATE community to build a system, where individuals own there data and have the right to decide with whom they share their data in different contexts, including mobility, healthcare, grocery and others. In that case, we need extremely secure, safe, and stable systems where the individual data is treated in a way that nobody can threaten them and application spaces can be protected. Maybe SENDATE could become a platform where this can be applied in new ways, not only between Finland and Sweden, but between Finland, Sweden, Germany and France.

Jon Simonsson, Deputy Director General at the Swedish Ministry of Enterprise and Innovation, VINNOVA, said that he is happy to see that the five partner countries have joined forces to be part of an open innovation system creating an open arena where industries, public sector and universities can cooperate and integrate new technologies together. He underlined that the public sector in Sweden is very important and that this sector has become part of the testbed notion to allow much more experimentation than what has been done up to now. In this context, Mr Simonsson said that international openness is very important for Sweden. He considers the SENDATE project to be a great example of an international cooperation that VINNOVA is keen to fund.

■ Further information is available on the SENDATE website at http://www.sendate.eu

Celtic-Plus Proposers Days in Istanbul and Leuven

Peter Herrmann
Celtic-Plus Office
herrmann@celticplus.eu

In autumn 2016, Celtic-Plus held two proposers days: on 22 September in Istanbul, co-organised with the help of the Turkish funding agency TUBITAK and hosted by ITU; and on 23 November in Leuven, co-organised and hosted at imec, a major Belgian research organisation.

Celtic-Plus Proposers Days have mainly three purposes: inform potential proposers about public funding opportunities, discuss potential ideas for Celtic-Plus project proposals, and network with potential project partners.

Istanbul Proposers Day

For the Proposers Day in Istanbul, 150 people had registered. The host, ITU, provided a perfect local organisation for open and constructive discussions. In his opening statement, Memet Aslan, Technology and Innovation Funding Programmes Director at TUBITAK, stressed the importance of Celtic-Plus for Turkey.

Erdem Ergen from KoçSistem, who represented the CoMoSeF project on Co-operative Mobility Services of the Future, reported in his keynote about the large societal and commercial impacts of CoMoSeF in Turkey.

Mete Karaca informed the audience about the Turkish Celtic-Plus framework and the improvements in public funding. TUBITAK announced an important simplification of their national evaluation process. The Turkish national evaluation of new incoming proposals will be based on the labelled Celtic-Plus project proposal document that was previously evaluated by industry experts. This will avoid time consuming and costly translation of the document into Turkish by the proposers. TUBITAK's announcement was positively received by the participants of the Proposers Day.

Mehmet Aslan, Director at TUBITAK

Many of them considered this to be an important simplification of the evaluation process.

All three Turkish Celtic-Plus Core Group Members gave a presentation about the research and business interests of their companies and showed their current and past activities in Celtic. The presenters of the Celtic Core Group were Riza Durucasugil from Netaş, Bulent Kirval from Turkcell, and Mustafa Ergen from Turk Telekom.

One of the core elements of the Proposers Day was the presentation of 13 interesting project idea pitches, which were well received and thoroughly discussed.

Among the presented research ideas are 5G-related networks, IoT technologies big Data and applications.

The presentations are available at https://www.celticplus.eu/event/celtic-plus-proposers-day-in-istanbul/

Participants at the Proposers Day in Istanbul

Leuven Proposers Day

For the Proposers Day in Leuven, 50 people had registered. The host, imec, provided a perfect local organisation in the imec Tower. Celtic-Plus Chairman Jacques Magen welcomed the participants, followed by imec Program Director Thomas Kallstenius, who presented his research organisation.

Steny Solitude from Perfect Memory, who represented the MediaMap+ Project on Media Management from Acquisition to Publishing, reported in his keynote about the impacts of the project for his start-up company.

Mathilde Reumaux informed the audience about the funding conditions of Innoviris for organisations from the Brussels region, and Danny Van Steenkiste explained the new funding agency VLAIO and the funding conditions for organisations coming from the Flemish part of Belgium.

Another core element of the Proposers Day was the pitching of seven interesting project ideas that were presented by participants from Belgium, Finland, Germany, and Turkey. The Celtic Office added a summary of the Istanbul project pitches and a selection of the pitches from Stockholm. Intense discussions followed the presentations and it was reported that this resulted in some deeper discussions that could lead to Celtic project submissions in the next call in April.

Among the presented research ideas are 5G-related networks, safer software development methods and an interactive programme guide for multimedia applications.

The presentations are available at https://www.celticplus.eu/event/celtic-plus-proposers-day-in-leuven-belgium/

Thomas Kallstenius, imec, Program Director Distributed Trust

SIGMONA – Software Defined Mobile Networks

Jari Lehmusvuori
Nokia Bell Labs
jari.lehmusvuori@nokia-bell-labs.com

Traffic volumes in mobile networks are increasing and end-user needs are changing rapidly. Mobile network operators need more flexibility, lower network operating costs, faster service roll-out cycles and new revenue sources for their 4G (LTE) networks. A key network solution is software-defined networking (SDN) with network functions virtualization (NFV).

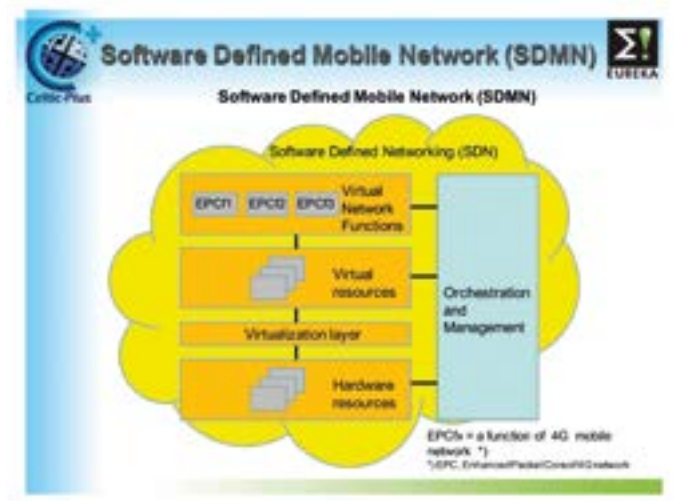
The research project SIGMONA successfully applied these novel technologies in the mobile networks. The project ended in April 2016. This innovative project realized multiple experimental systems and showed exciting demonstrations of these technologies that will change the world of communication.

The changing market

End users expect fast connections and high-quality services for their smart phones at any time and any place with affordable pricing. In addition, the ICT market, including the mobile networks, is shifting from dedicated hardware to software, including open source software, and cloud technologies which, with SDN, will change the mobile core network. The transformation means migration of application software from proprietary, application-specific hardware platforms to virtualized compute servers deployed in a few large-scale data centers.

Flexible end-to-end network architecture for LTE (4G)

SDN integrated in the mobile network with OpenFlow protocol implies the separation of the control plane from the data plane in networking equipment. NFV refers to executing the control and management plane functions in virtual machines or containers using cloud computing. The mobile network architecture is considerably changed to optimize for the virtualization and cloud computing principles as shown in the Figure. This approach adds flexibility and supports the gradual introduction of high network throughputs, optimal flow management, and traffic engineering possibilities.



Software Define Mobile Network concept with virtual resources and SDN.

Conclusion

The novel LTE/4G network architecture concepts with NFV and SDN were validated with test systems, and demonstrated for example in the Mobile World Congress 2015 and 2016.

New or improved products for the virtualized 4G/LTE networks emerged from the project results. A start-up company, Cumucore (www.cumucore.com), was established for business on a virtual 4G network.

Standardization contributions were provided to the major industry initiative on Network Functions Virtualization (NFV) in ETSI Industry Specification Group (ISG) NFV. Open Source software was submitted to OpenStack cloud platform.

A very high number of publications and conference presentations highlight the academic qualifications of the project work. A book on the Software Defined Mobile Networks (SDMN) was edited and published (Wiley ISBN-13: 978-1118900284).

SIGMONA, among other related research projects, has provided a solid baseline on NFV and SDN for the 5G research in-progress, for example in the EU H2020 projects.

A White Paper was made to summarize the key results of the project. The White Paper, as well as the research Deliverables, can be found on the project website at www.sigmona.org.

The SIGMONA project, run at the same time as the industry initiative ETSI ISG on NFV, was in the position to provide research results in time for the major mobile networks transformation that is taking place.

- Further information is available on the project page at https://www.celticplus.eu/project-sigmona/

TILAS – Large-scale urban IoT deployments

Aránzazu Sanz
TST
asanz@tst-sistemas.es

TILAS concept for large-scale Smart City deployments

The Internet of Things (IoT) is becoming a mature technology, and it plays a key role in the urban context. Both efficiency and sustainability are fundamental concepts, which have driven the evolution of cities towards a new dimension. In this evolution IoT plays a core role, which has been assessed in the TILAS project.

Predictions indicate that around the year 2050, more than 70 % of the world population will be concentrated in urban areas. Thus, city players are analysing how to address the new demands imposed by such a population concentration whilst guaranteeing a high quality of life. The goal of Celtic-Plus project TILAS (Technology improvements for large-scale Smart City deployments) is to provide solutions and guidance to the technical community for addressing massive IoT deployments in the urban context.

The initial experimental IoT deployments have revealed important missing components which are critical when facing a massive IoT deployment in hostile environments with no control on the environmental conditions, propagation behaviour or interference presence. The TILAS consortium has designed a wide number of innovative solutions to address the challenges linked to massive IoT deployments. All of them have been deployed on top of large-scale testbeds running in several cities and laboratories.

NO_2 and O_3 sensors deployed in the city of Santander, Spain

Approach and results

TILAS worked on different scenarios, use cases and business models to develop a system concept in which the corresponding innovations are covered and aligned with already existing IoT/M2M (Machine-to-Machine) standards. Among them it is worth highlighting the following ones:

- Customized housing embedding antennas aiming at overcoming visual impact problems.
- Robust multihop over-the-air programming (MOTAP) techniques aiming at easing network management and reconfiguration of large-scale IoT infrastructures.
- Design and implementation of a flexible hardware and software architecture aiming at accommodating the myriad of standards operating in the market.
- Design and implementation of a security framework.
- The design and implementation of a middleware able to feed the collected information to the applications running in the cloud.

Field trials and demonstrations

A vehicle traffic pattern monitoring platform based on NO_2 and O_3 sensors has been deployed in the city of Santander. The above developments have been tested on top of several devices, which have been integrated with the large-scale IoT platform running in the city.

The project has also supported additional activities in other cities, such as Seoul, in which – based on the contributions described above – a real-time water monitoring framework has been deployed. Last but not least, image/video surveillance was demonstrated in Paris, and the security framework has been assessed in the city of Grenoble linked to an environmental monitoring application.

Conclusion

The TILAS consortium has designed, implemented and assessed a number of practical tools, which will provide the basis for future massive IoT deployments. The cities participating in TILAS and several others have already showed additional interest in exploiting further urban services aiming at optimizing current performance.

- Further information about TILAS is available on the project page at https://www.celticplus.eu/project-tilas/

How Sweden manages the Celtic-Plus project process

Jessica Svennebring
Vinnova
jessica.svennebring@vinnova.se

Vinnova is the Swedish public authority for granting national funding of Celtic-Plus labelled international projects. As a EUREKA Cluster, Celtic-Plus is highly regarded in Sweden, because it is based on the principles of EUREKA, according to which both European and global participants are welcome in the projects. This article explains Vinnova's view on the benefits of Celtic-Plus and how Vinnova manages the process for getting the best out of Celtic-Plus projects.

Advantages of the Celtic-Plus programme

From a Swedish point-of-view, the main advantage of Celtic Plus is the bottom-up approach of the industry-driven projects, which is well in line

Figure 1: International networking through Celtic-Plus is appreciated by Swedish enterprises for its bottom-up, simple and agile process

with the strategy of Vinnova. For the participants, EUREKA clusters, such as Celtic-Plus, present an opportunity to expand their network and enter new markets.

Furthermore, the easy and simple administration of Celtic-Plus increases the potential of getting both large companies and SMEs interested in joining. For new Swedish participants entering a Cluster project for the first time, the well-organized and structured programme of Celtic Plus is appealing. Another advantage is the availability of standard project documents, like for example collaboration agreements regarding intellectual property and other complex questions.

Regular project evaluation and monitoring of ongoing projects ensure the highest possible value creation of the project. Also, most important, to mirror the rapid industrial development within telecoms, the pragmatic approach within Celtic Plus, allowing for easy change request processes resulting in an agile way of working, is both appreciated and required for successful project results.

SENDATE-EXTEND – a case study

Let us look at a recent example, the newly started Celtic-Plus project SENDATE-EXTEND. The acronym stands for "Secure Networking for a Data Center Cloud in Europe – extended data center solutions". The project is funded by Vinnova. The total cost is estimated to be 50.7 million Swedish crowns (5.3 million euro) over three years. The project involves both several large Swedish companies as well as academia and SMEs. SENDATE-EXTEND will take a holistic approach on automation of control, management and orchestration across the different layers of a data center, as shown in Figure 2.

Continuous improvements of efficient national funding process

Vinnova, as the Swedish public authority, has a central budget for all EUREKA Clusters. It means that all labelled projects in Celtic-Plus also compete against projects with a label from other EUREKA Clusters. The internal review process includes a Swedish board of experts and often interviews with all candidates. Important factors in these discussions are the Swedish aspects of future growth potential, value creation and local attractiveness within each project.

At Vinnova we strive for simpler and faster processes in order to give the highest quality and service to our customers, the applicants. For the cluster partners the time is running fast, and to shorten the time to grant, Vinnova is focused on ensuring that our internal processes are continuously improved and made more efficient.

During the last years, the number of applicants has increased, and this is a very positive trend, showing the increased awareness of the importance of industry-driven funding alternatives.

Conclusions

From a Swedish perspective, the main advantages of Celtic-Plus is the industry-driven bottom-up approach of the programme, the simple administration and the pragmatic process concerning change requests for a running projects. All of which defines an agile structure allowing businesses to follow the current market evolution. In this context, Vinnova is focused on delivering an efficient national funding process for our customers, the applicants.

The newly started Celtic-Plus project SENDATE-EXTEND, funded by Vinnova, is an excellent example of the fruitful collaboration between several Swedish players, including large companies, academia and SMEs.

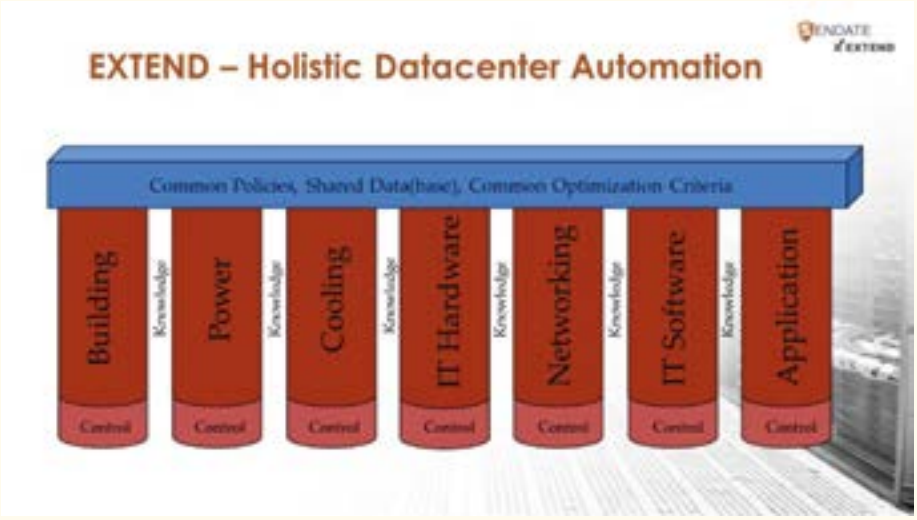


Figure 2: SENDATE-EXTEND is focusing on cross-layer automation and monitoring in data centers

SHARING – SMart Advanced Radio Technologies for 4G networks

Arturo Ortega Molina
Orange
arturo.ortegamolina@orange.com

The SHARING project was created to stimulate the 4G evolution towards 5G mobile networks by developing innovative technologies designed to improve network performance and user experience.

Main focus

The SHARING project defined reference scenarios and explored new concepts with a special focus on interference management, cost-power efficient small cell deployments, LTE-A / WiFi convergence, network-controlled device-to-device communications, meshed relay-assisted networks, Self-Organized Network (SON) features and architecture evolutions for heterogeneous networks.

The project's main achievements include, among others: (1) rationale and forecasts (2015-2020) for worldwide and European small cells, carrier WiFi, D2D and relay markets; (2) advanced techniques required to cope with traffic increase, and to fulfil the objective of "services for everyone everywhere" such as coordinated multi-point, advanced receivers and carrier aggregation; (3) methods that can significantly reduce (up to 50%) average network energy consumption while still maintaining the desired quality of service; and (4) a software solution designed to improve user localization in heterogeneous 3GPP / WiFi networks. Impact on network architecture of all project innovations was assessed giving a hint on compatibility with current standards and implementation straightforwardness.

Approach

SHARING aimed to achieve a major capacity increase by leveraging on:

- Advanced Self-Organizing Network (SON) mechanisms and advanced cooperation technologies.
- Multi-layer and multi-RAT offloading of macrocell traffic to (a) outdoor small cells, (b) indoor femto cells and Wi-Fi, and (c) enabling Device-to-Device (D2D) communications.
- A flexible interference management approach combining the advantages of interference avoidance and interference cancellation.

Achieved results

SHARING developed innovations which consolidate small cell-technologies related to heterogeneous multi-RAT and multi-layer networks. These innovations are in the following areas:

- Flexible air interface consisting of multi-point coordination transmitters, interference cancelling receivers and coordinated interference management tailored for future heterogeneous networks.
- Novel strategies for seamless intra- and inter-RAT traffic offloading.
- Self-organized methods for managing mobility, interference, spectrum and radio resources.
- Fronthaul solutions covering advanced relaying and device-to-device communications.
- Heterogeneous network architecture enablers needed by device-to-device communications.

The project also developed cost-efficient technologies and solutions, namely:

- Effective interference mitigation and management in heterogeneous networks.
- Smart and efficient traffic steering strategies taking into account the actual operational conditions.
- Innovative cost effective fronthaul architectures for heterogeneous networks.
- RF front-end (reconfigurable energy efficient power amplifier and miniature frequency agile antenna), as enablers for Carrier Aggregation.

SHARING contributed to taking current offload solutions to next-generation smart Multi-RAT HetNets, thereby contributing significantly to eco-

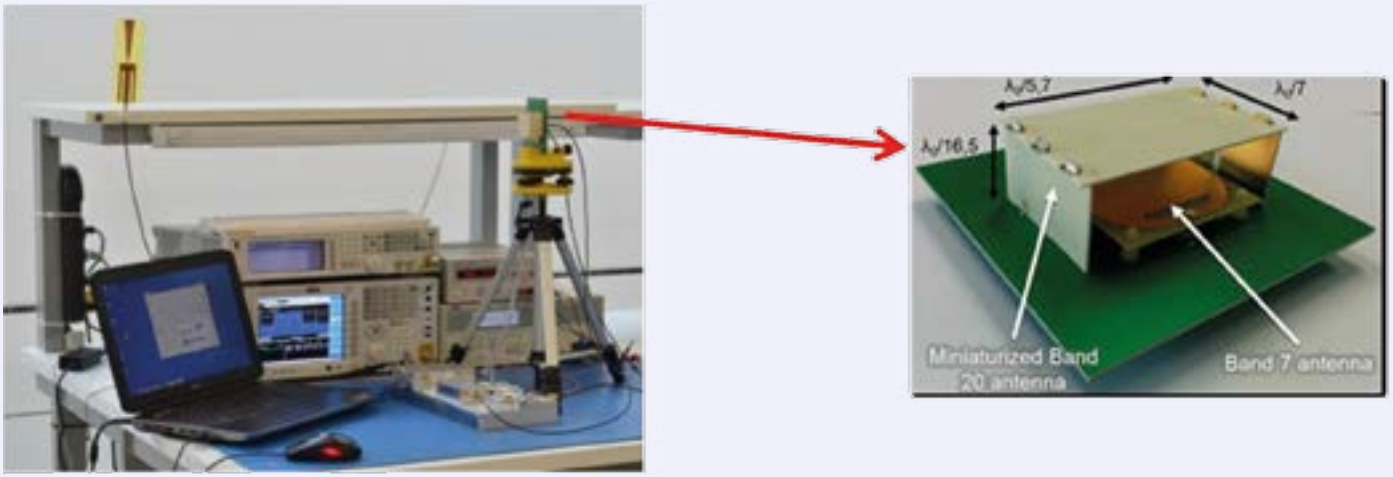


Figure 1: Carrier aggregation demonstrator setup comprising the reconfigurable RF front-end (including a dual band miniature antenna), the control PC and the measurement equipment

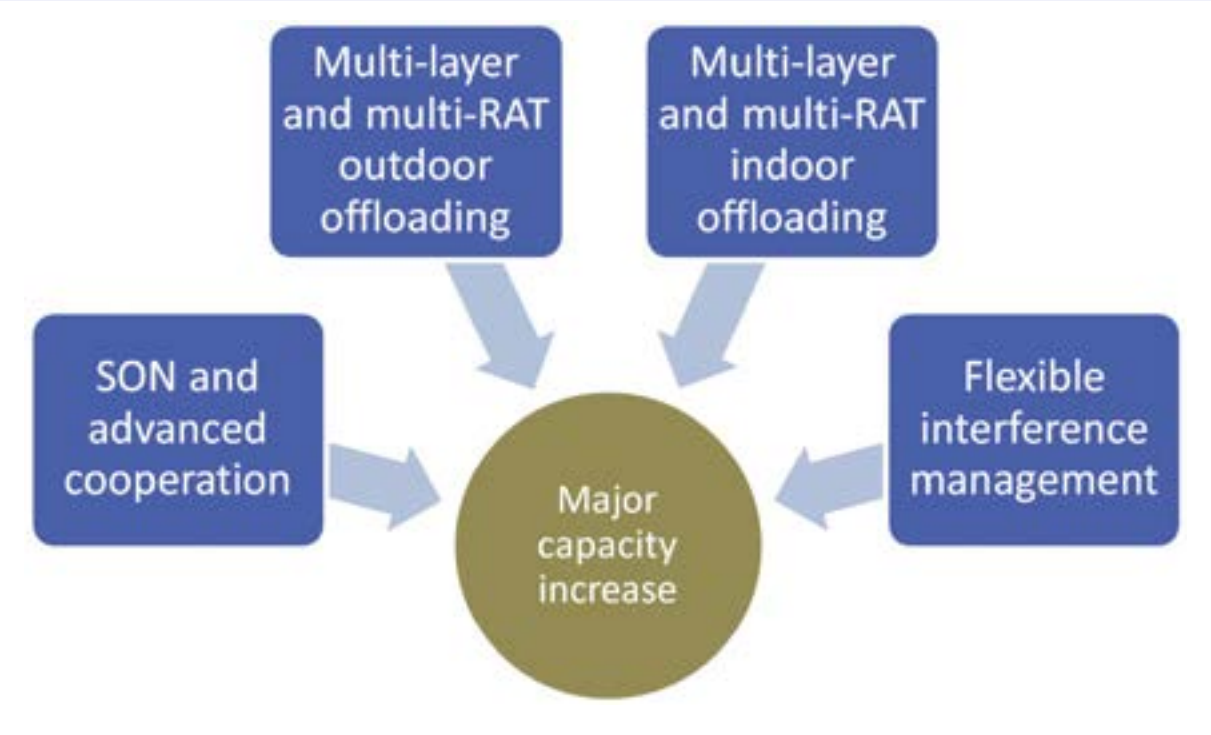


Figure 2: SHARING overall target

nomic and energy-efficient access networks.

Impact

During the SHARING project the focus in 3GPP was on finalizing Release 12 and initiating the Release 13 specifications of LTE-Advanced systems. Some of 3GPP activities that are the most relevant to SHARING project are device-to-device communications, interworking between LTE and WLAN, ON/OFF energy savings and small cells. The project contributed to 29 technical contributions for 3GPP RAN1, RAN2 and RAN3.
SHARING also contributed to the improvement of a significant variety of products including power amplifiers, dual connectivity solutions, interference cancellation chipsets, relaying and carrier aggregation solutions, radio propagation models, and RF fingerprint positioning platform, and seamless multi-RAT connectivity solutions.
A great deal of effort was also spent on dissemination activities leading to a significant number of publications in prestigious conferences (78), journals (33) and workshops (11); and to the organisation or co-organisation of 6 workshops or special sessions. The project has also issued 1 book and has obtained 2 best paper awards.

- Further information is available on the SHARING project website at http://www-sharing.cea.fr

Celtic-Plus
Smart Connected World

www.celticplus.eu

About Celtic-Plus

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new "Smart Connected World" paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the inter-governmental EUREKA network. Celtic-Plus is open to any type of company covering the Celtic-Plus research areas, large industry as well as small companies or universities and research organisations. Even companies outside the EUREKA countries may get some possibilities to join a Celtic-Plus project under certain conditions.

EUREKA

Self-protection against botnet attacks

Solutions by 5G PPP project SELFNET

Manuel Gil Pérez
University of Murcia, Spain
mgilperez@um.es

Giacomo Bernini
Nextworks, Italy
g.bernini@nextworks.it

Cyber-attacks can affect both continuity and delivery of services. Such attacks threaten to directly affect subscribers of emerging 5G services. To protect them, 5G PPP project SELFNET has developed solutions particularly aimed at botnet attacks.

According to a statement from July 2014 by Joseph Demarest, Assistant Director in the Cyber Division at FBI, 18 computers per second are globally infected by a botnet. Botnets are one of the most powerful cyber threats subverting communication links. [1] That highlights the importance of detecting and dismantling botnets in any type of communications network. But in 5G, botnets pose an even greater security-related challenge due to the expected large number of connected devices with high mobility capabilities.

The detection and mitigation of botnets for improving security in 5G networks is the main goal defined in the self-protection use case of SELFNET (Framework for Self-Organized Network Management in Virtualized and Software Defined Networks) [2]. SELFNET is a Horizon 2020 project under the 5G PPP programme, which is devoted to designing and implementing an autonomic network management framework to achieve self-organizing capabilities in managing network infrastructures.

Enabling self-protection capabilities against botnets in SELFNET

The self-protection use case is designed to demonstrate the self-protection capability of the SELFNET solution in detecting and isolating compromised devices, also known as zombies, which constitute a botnet.

In a first step, the detection of a given botnet has been divided into two different detection phases, at two complementary levels of abstraction. In a first Self-Organizing Networks (SON) control loop, possible zombie devices are detected by identifying Command & Control (C&C) channels. These channels are discovered by analysing the network flows exchanged between the zombies and the C&C server, the botmaster in charge of controlling the zombies. As the type, size, and number of packages exchanged in a given period of time between the C&C server and different zombies is very similar, our solution is able to detect possible zombies. This SON control loop is due to the large number of connected devices expected in 5G networks, making it not possible to analyse all the traffic flooding the network.

Once a zombie is identified as a potential compromised device involved in a botnet, a second SON control loop of detection is carried out. In this case, fine-granular detection at low-level (Deep Packet Inspection, DPI) is required to ensure the existence of those C&C channels.

In SELFNET, this second phase is performed by a DPI tool like Snort, which is dynamically configured by SELFNET as a sensor. That dynamicity is a must, because 5G subscribers, as entities with mobility capabilities, will be moving around the network, thus changing their network settings (mainly their IP address) constantly. Due to that, the detection tools (Snort in this case) will be updated by SELFNET to continue performing their detection tasks on these mobile devices.

As a reaction to the previous detection, a virtualized and personalized honeynet is being configured as an actuator network function, in order to isolate potential cyber-attacks such as Distributed Denial of Service (DDoS) attacks, which can be triggered by the botnet owner. Such a honeynet acts as a fake network: the detected zombies are logically placed as cloned zombies to emulate the behaviour patterns of each real zombie, by contacting the C&C Server, the main dashboard of the botnet owner, on behalf of the real, original zombie. From that moment on, the botnet owner will believe that the real zombie still exists, although it is not true. Subsequent cyber-attacks will not be carried out in reality.

Proof-of-concept prototype of the Self-Protection use case scenario

A proof-of-concept prototype demo of the primary self-protection use case scenario has been recently developed. This demo consisted of the following three steps:

Step 1. Traditional mode: SELFNET does not come into play.
A new zombie is recruited in a botnet, which is used to trigger an HTTP Flood attempt (DDoS at-

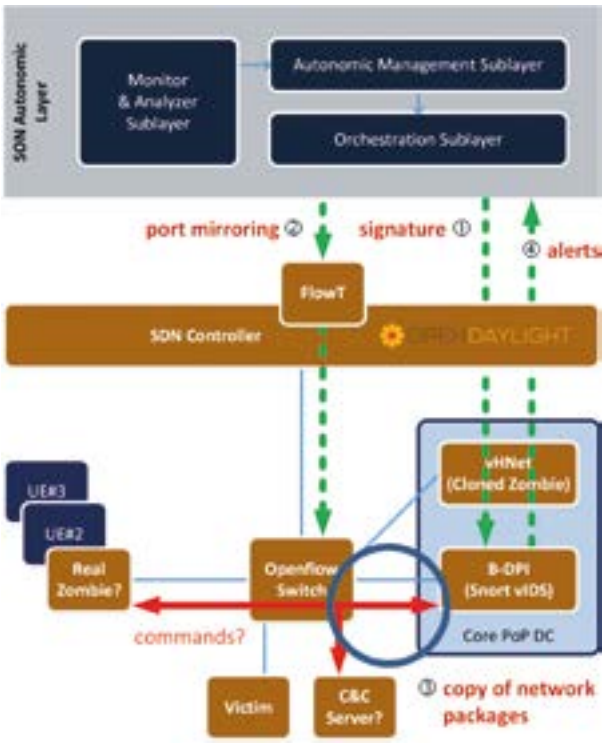


Figure 1: Proactive confirmation of a botnet through a DPI process

tack). This first step demonstrated, which problems a potential botnet could cause via a zombie launching a DDoS attack against a given victim.

Step 2. A suspected user end (UE) is detected as being part of a botnet (see Figure 1).
A DPI tool (Snort vIDS) is configured with a detection rule or signature to confirm that the suspected UE is an actual zombie. After that, a new flow rule is added into the virtual switch to enable the port mirroring feature, in order to send a copy of the raw network packets to Snort to be analysed.

As a result of this step, Snort will be able to generate alerts in IDMEF in case the UE is an actual zombie.

Step 3. A honeynet is configured to isolate the zombie communications to the botnet (see Figure 2).
This flow is diverted to the honeynet, named Traffic Diversion in Figure 2, in order to avoid the execution of a potential DDoS attack.

If the same HTTP flood attempt conducted in the first step is executed again, the victim will be not threatened by the attack. The victim is now protected by the SELFNET solution.

It is worthy to note that the demo showed the detection and mitigation of cyber-attacks conducted by a botnet in a proactive way, disabling the zombies' malicious behavior before they can be used as sources of a cyber-attack. The detection of 5G subscribers' devices as suspected zombies is defined in the Self-Protection use case of SELFNET, carried out through a first SON control loop, which was outside the scope of this first proof-of-concept prototype demo.

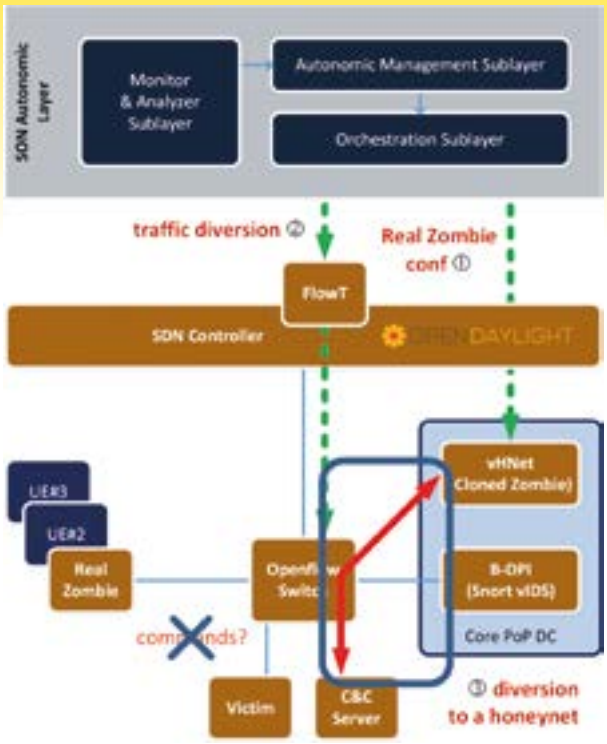


Figure 2: Isolation of compromised devices in a personalized and virtualised honeynet

Conclusion

The solution proposed in the self-protection use case of the SELFNET project is able to detect and mitigate botnets in 5G networks. This proposal discovers C&C channels and therefore zombies using a detection process composed of two different phases. The first one is a low-granularity loop in charge of detecting possible zombies analysing network flows. Once the possible zombies have been detected, the fine-granularity loop uses DPI tools to analyse the packages exchanged between the possible zombies and the C&C server. Finally, the reaction process consists of creating a virtualized honeynet where potential cyber-attacks such as Distributed Denial of Service (DDoS) are isolated. In order to demonstrate the usefulness of our solution, we deployed a proof-of-concept prototype demo where the detection and reaction phases are shown.

As future work, and due to the high mobility of users in 5G networks, we plan to consider the users' location and their mobility in the detection and reaction processes. Specifically, when zombies and C&C servers move across different networks, it is required to identify and process locations in order to continue detecting and mitigating future attacks.

References

[1] Joseph Demarest, "Taking down botnets: public and private efforts to disrupt and dismantle cybercriminal networks." Statement before the Subcommittee on Crime and Terrorism, United States Senate, July 2014. URL: http://www.judiciary.senate.gov/meetings/taking-down-botnets_public-and-private-efforts-to-disrupt-and-dismantle-cyber-criminal-networks

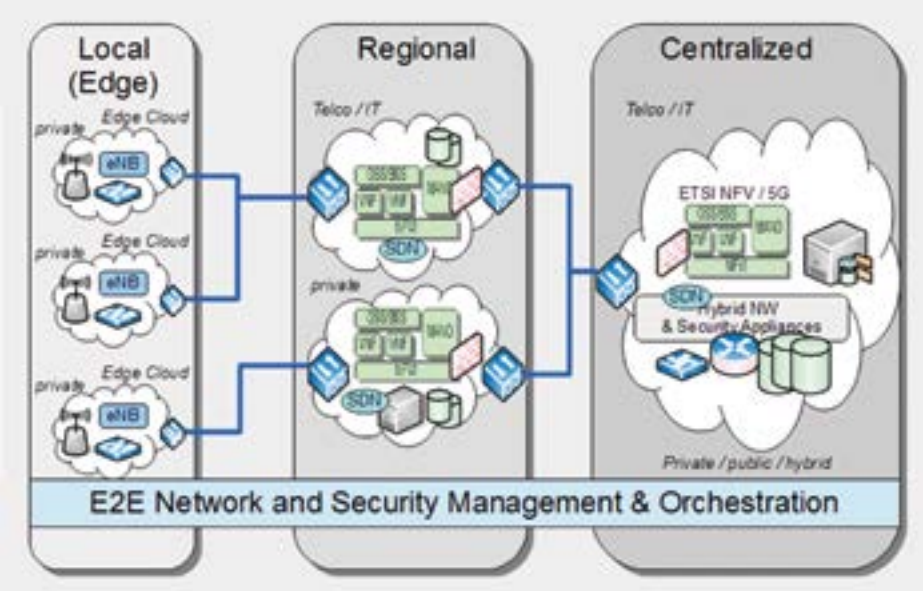
[2] SELFNET – Framework for Self-Organized Network Management in Virtualized and Software Defined Networks, URL: https://selfnet-5g.eu/

Security of distributed datacenters

Celtic-Plus project SENDATE-PLANETS

Dr. Manfred Schäfer
Nokia Bell Labs, Security
manfred.schaefer@
nokia-bell-labs.com

SENDATE-PLANETS is a sub-project of Celtic-Plus project SENDATE. In PLANETS, European partners examine architectural, networking, security, and security management aspects of distributed datacenters and underlying technologies – including Virtual Network Functions (VNF), Software Defined Networking (SDN), and virtualization techniques.



Security management across distributed datacenters

The SENDATE project (2016 – 2018) aims at scientific and technical concepts and solutions for secure and flexible low-latency and locality-aware distributed datacenter approaches, integrating with SDN-based high-speed transport networks. It envisages upcoming application scenarios, such as Industrial Internet, mobile connected objects, Internet of Things, health applications, and 5G, while specifically advancing security.

In datacenters sensitive business and private data is stored, processed and forwarded. Current datacenters offer enormous computational power and storage capacities, but they are located far away from customers, use networks only for transport, and are mostly run by non-European companies. This leads to low flexibility, long delays, and manifold security concerns.

Security research in PLANETS

Based on strengths and expertise of European partners in security and in virtual network technologies, essential shortcomings and vulnerabilities of today's distributed datacenter approaches shall be prevented. Consequently, security work in SENDATE-PLANETS is focused on intra- and inter-datacenter security, security related management, orchestration, and analysis, embracing placement, integrity, and security lifecycle management of VNF, as well as of high speed transport networks to trustworthily interconnect servers in a datacenter, datacenters among each other, as well as end users. With upcoming technologies (like Network Functions Virtualization NFV and SDN) new attack vectors arise, which must be countered with adequate security controls.

New risks and challenges

One reason for new threats is the shift from dedicated, traditional Hardware (HW) with encapsulated security mechanisms and secrets (protected by crypto-processors, firmware, or security-designed embedded systems), stable network topologies, and solid security appliances (firewalls, proxies, security gateways – HW boxes in proprietary premises, shielding against unauthorized access) towards virtualized SW (like VNF) instantiated on standard HW, which may reside in less secure environments of huge, distributed datacenters and temporary edge clouds.

Techniques for software isolation, traffic separation, and resource management in virtualization platforms, operating systems (OS), and hypervisors are highly sensitive and potentially vulnerable.

For example, container based virtualization (CBV) is gaining ever greater significance, while competing with traditional hypervisors and heavy, fully-bootable virtual machines on top. However, CBV does neither use horizontally intercepted nor HW supported virtualization. Instead, containers share one (huge) Linux kernel, which isolates containers and their resources via fine-granular kernel-level data and control structures. Compared to hypervisors, dependencies from kernel code and vulnerabilities are much higher, and security configuration becomes complicated and error prone.

Mobility and dynamicity of VNF together with limited protection for critical secrets, code and data in SW and difficulties to ensure uniqueness, confidentiality, and integrity, raise additional risks and thus, enable new chances for cyber-attacks. Additionally, organizational security policies may demand specific geo-locations for VNF, binding of VNFs to individual security clusters, or even to HW with defined security capabilities.

On service level, tenant separation and segmentation of distributed services and traffic is essential, having many impacts on the underlying virtualization and network technology. Moreover, new challenges arise for establishment of security domains and clusters, particularly, when realized across several infrastructure domains.

Modern devices implement open, vulnerable SW applications and OS, and partly even allow firmware-level modifications – resulting in significantly higher risks for users, data, and control planes. Specifically in the IoT area, different and lightweight methods for network access arise, competing with well-established, secure SIM/USIM-based technologies.

It is conceivable that new forms of malware will occur, promoted by oodles of devices of mixed type – with different security capabilities and challenging vulnerabilities. Thus, the need to flexibly detect malicious traffic and behavioural anomalies will significantly increase.

To guarantee a sufficient level of security, systems and services must dynamically fulfil security SLAs and policies. This requires a high degree of seamless, automated SM over distributed datacenters, enabling immediate responses to critical security events. Beyond that, security life cycle management for VNF and for distributed services must be supported, requiring continuous SM for security adaptions of service changes (e.g., adapting firewall rules, whenever moving a VNF), hardening of VNF and platforms, as well as traffic and event monitoring and analysis – across the virtual and physical architectures, domains, and network topologies, as combined for service distribution.

Security subjects under examination

Parallel to designing a new, clean-slate SENDATE-PLANETS network architecture and relevant use cases, upcoming risks will be evaluated, and necessary security mechanisms and SM methods will be developed to protect network technologies and new service types. To increase achievable security levels the technologies themselves, especially virtualization platforms and SDN, will be enhanced with efficient protection mechanisms. Essentially, the partners will contribute to:

Virtualized environments

Concepts for secure runtime environments for SDN/VNF applications will be developed, reflecting identified security requirements, such as multi-tenancy. In focus are isolation methods for CBV and other virtualization techniques and for securing communication of applications and management components.

Likewise, security capabilities of existing virtualization approaches will be examined. It will be investigated how Virtual Machine Introspection techniques can be lever¬aged, e.g., to enable anomaly detection.

Datacenter Security Management (SM)

Essential SM aspects will be considered, including security for the inter-operability of distributed datacenters, continuously protecting network infrastructures and SM entities. A second scope is holistic, security policy based and dynamic SM and orchestration for domain/cloud-crossing services, e.g., automatically inserting security functions, adapting security configurations, and exploiting cloud elasticity to fulfil associated security policies.

Partners will investigate methods for inter-domain security information exchange, including a multi-tenant capable Inter-Domain Network SM System for NFV-/SDN-based high throughput networks, and for validating properties of SW and configurations of SDN functions and development of tools, automatically assessing compliance with security properties, like tenant separation.

Research work also comprises: secure, resilient solutions for telecom and IT cloud implementations, a new group communications (GC) solution – factoring in the latest technologies (like SDN) and evolution in standards (e.g., 3GPP), development of tools supporting forensics analysis, including backend support, validation and integration into forensics-related processes.

Moreover, baselines of device identity management and organizational possibilities will be studied, embracing comprehensive data models for non-human identities.

High Security Networks and Nodes

Integration of Network Intrusion Detection Systems (NIDS) with SDN-based high-speed networks will be investigated, too. SDN and NIDS techniques are combined to increase network security and to analyse SDN support for flexible NIDS deployment.

For increased safety, development of demonstration prototypes for typical security applications of HW security modules and protected security processors is envisaged, concentrating on tamper-resistant security mechanisms for measuring HW and SW integrity, on digital signatures to detect illicit changes of data structures, on data encryption, and on chip-integrated PKI to secure system interconnection and to manage keys and certificates.

Partners implement proof-of-concepts of an NG network building block for SDN-based networks, combining different technologies (FPGA, TPM, SDN, Micro Kernels,...). Several usage scenarios are considered, including a hybrid combination between a switch and a fully-fledged application level gateway, building the building block as trustworthy unit, usage of highly secure hypervisor in L4 technology, FPGA support for reconfigurable data planes, etc.

Further investigated are methods and tools for monitoring, incident response, logging, and automatic detection of exceptional behaviour, advanced security methods for Ethernet based IT infrastructures, modules for adaptive risk management including intrusion detection functionality, response and forensics, data-on-rest encryption solutions, automated verification and validation of adaptive responses of the SDN network caused by network traffic, and high security PMR radio network elements in a virtualized SDN architecture.

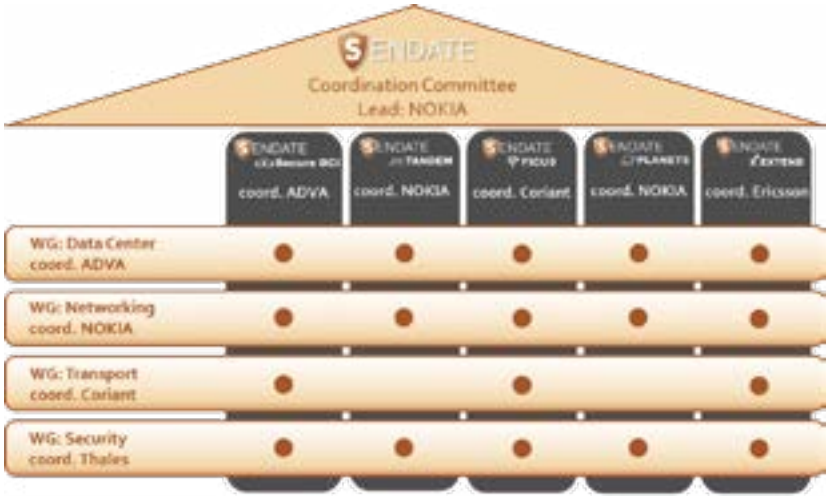
Secure architecture and lifecycle for M2M applications

An architecture for M2M applications will be defined to ensure security functions for M2M-services over the life cycles of deployed systems. Operation-critical M2M-services will be considered, connected to, e. g., wireless IoT nodes, control loop peers and virtual entities in datacenters. Partners will study wireless sensor networks (WSN) and their security aspects, particularly the applicability of IPv6 to WSNs, as well as methods for IoT security and real-time attack detection for networked devices in home environment.

Outlook

Major results of the three-year project PLANETS will be available in 2017. Essentially innovations can be expected, providing abilities to fully control and analyse the overall security infrastructure of distributed datacenters and to maintain integrity and security of VNF and SDN based solutions. Reinforced security concepts will bring new opportunities for the European industry, strengthening their position in essential areas of security for network virtualization.

Further information:
SENDATE website: http://www.sendate.eu
SENDATE-PLANETS website: https://www.celtic-plus.eu/sendate-planets



Enabling the 5G ecosphere

Second Global 5G Event in Rome

Uwe Herzog
Eurescom
herzog@eurescom.eu

The Second Global 5G Event took place in Rome, Italy, on 9-10 November 2016. The motto of the event was "Enabling the 5G ecosphere". With 350 participants attending it attracted a large number of participants from Europe and all over the world. But the conference was also attractive in terms of high-profile speakers and an interesting exhibition.

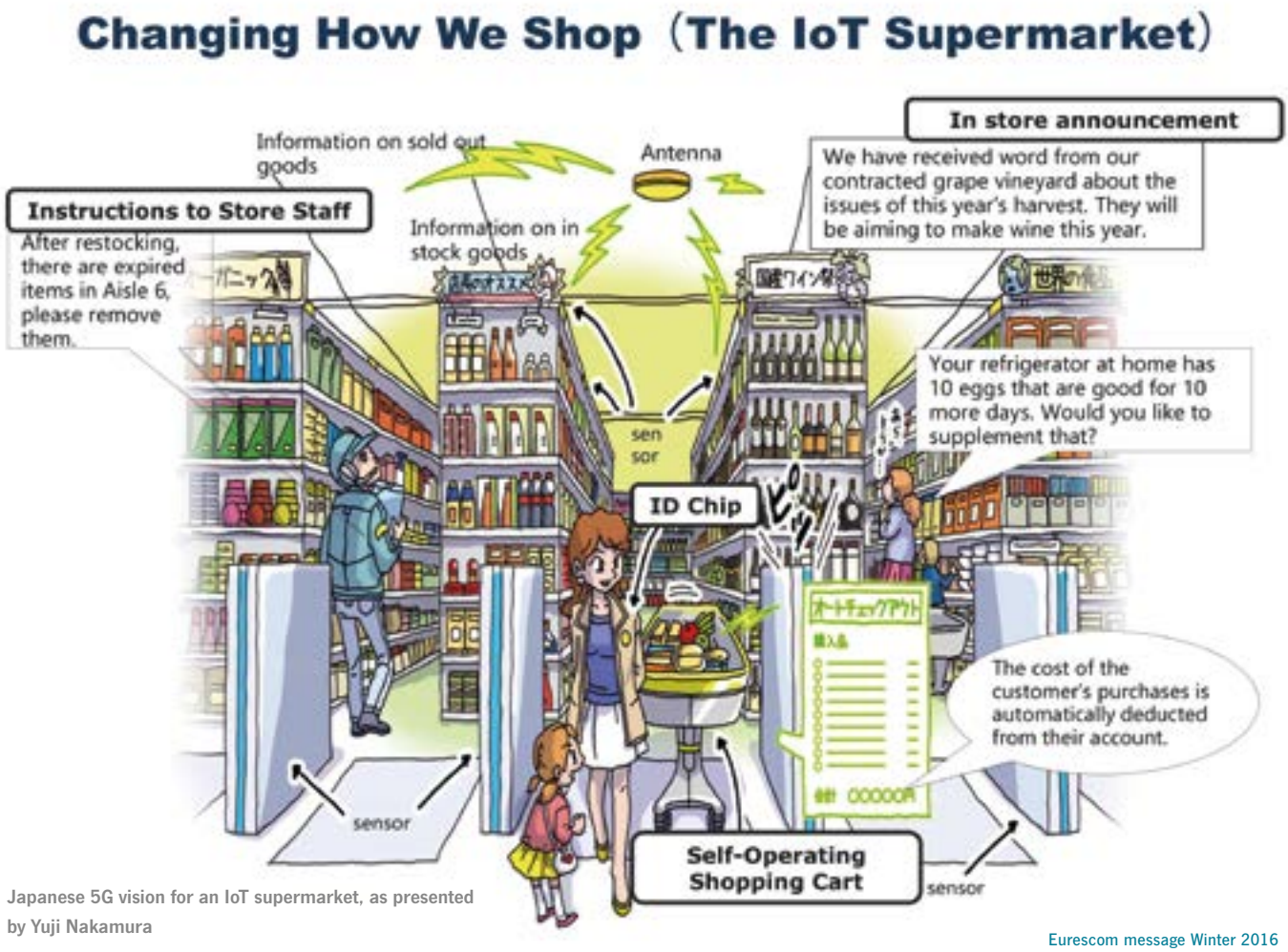
Leading global 5G associations from the world's regions came together to offer the second of a series of Global 5G Events in Rome on 9 and 10 November 2016. This series of events is based on a Memorandum of Understanding to cooperate on building global consensus on 5G that was signed in October 2015 by the five organisations in the world that are driving 5G. These are the 5G Infrastructure Association (on behalf of the European 5G PPP), 5G Americas, (Americas), The Fifth Generation Mobile Communications Promotion Forum – 5GMF (Japan), 5G Forum (Republic of Korea), and IMT-2020 5G Promotion Group (China).

The first time the event was hosted in Europe

After the first event was held in China in June 2016, this time it was Europe's turn to host and organise the event. The event was opened with a welcome address by Antonello Giacomelli, Undersecretary of the Minister of Economic Development, representing the Italian Government. He revealed some news that even insiders in 5G research in Italy were not aware of, namely that the Italian Government has decided to set up and run 5G pilots in three Italian cities by 2018.

Undersecretary Antonello Giacomelli

In the sessions of the event, experts from all corners of the globe discussed 5G progress through a series of focused sessions on 5G policy perspectives, 5G system architecture, spectrum, 5G air interface and radio resource management, network management & software networks and 5G for verticals in the new economy.



Japanese 5G vision for an IoT supermarket, as presented by Yuji Nakamura

The policy view

In opening session 1 on policy views, representatives from all five regions explained their view of 5G research and deployment aspects: From the European Commission, Director General Roberto Viola revealed plans that EC plans to define corridors in Europe, from East to West and From South to North, in which innovative technology can be deployed and tested e.g. for testing autonomous driving and of course these corridors will also be available for deploying 5G pilots. In China, 5G Technology R&D trials will take place in 2016-2018 with international involvement, followed by product R&D trials 2019-2020 and 5G launch in 2020. For Japan, Yuji Nakamura explained that 5G implementations are planned to be ready in 2020 for the Olympic Games Japan. He sketched a few interesting scenarios for how 5G could change our lives – see the figure of the IoT supermarket.

Julius Knapp, US, FCC, focused his speech on spectrum the aspects. He talked about what spectrum US government is making available for 5G in three bands, calling it the "Spectrum trifecta". It is a combination of re-devoting spectrum (e.g. 700 MHz TV incentive auction), facilitation of spectrum sharing (e.g. 3.550-3.700 GHz) and new spectrum in mmW bands of which the last apparently receives strongest interest by US industry.

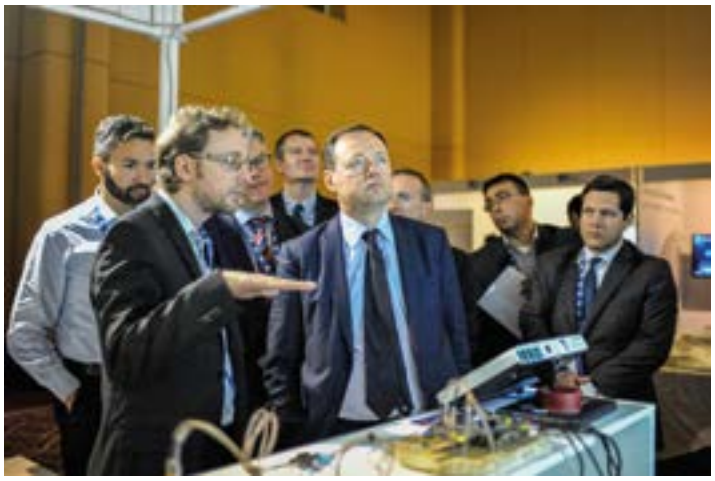
Spectrum is the lifeblood of our industry

The industry perspectives session was opened by a welcome address from TIM Executive Chairman Giuseppe Recchi. After him, the presenters from the 5G fora spoke about roadmaps towards the implementation of 5G, about spectrum and e.g. requirements from User Scenes. Kohei Satoh, 5G Mobile Forum, said that 5G will not need to always achieve its maximum performance in all instances, but provide it related to the scenario and its requirements, e.g. for high energy saving, high mobility or high capacity, respectively. Chris Pearson, 5G Americas, said that in his view 5G will not only transform networks but also industries. He said that for Smart Cities a market size of 757 billion US dollar is expected for 2020, and other relevant markets were transportation and remote medicine. He said that "Spectrum is the lifeblood of our industry", and that one should simply "put the spectrum out in the market and let the industry drive innovation".

EC plans industry-led venture fund

At the end of the first day, Commissioner Oettinger informed the audience that the EC plans to launch an industry-led venture fund of 500 million euro. He made it clear that the EC expects a globally harmonized 5G solution: "Defining individual 5G solutions prior to reaching a global consensus is not appropriate and will not benefit anyone". He also reminded the audience that decisions about spectrum will be made at the World Radio Conference, WRC 2019: "We should ensure that regional decisions on spectrum will not jeopardise a global solution".

TIM executive chairman Giuseppe Recchi in front of the audience



EC Director General Roberto Viola (centre) visiting the exhibition

Architecture, spectrum, 5G air interfaces and 5G vertical sectors

A number of further sessions took place on the important elements of a 5G system. High-profile speakers from industry, standards bodies, fora and vertical sectors provided excellent insights on the current status, plans and inspiring ideas. For everyone who did not have the chance to attend the event it might be worth going through the presented slides, most of which can be downloaded from the event website (see link below).

Conclusions and next event

In the final session, Werner Mohr, Chairman of the Board of the 5G Infrastructure Association, summed up the event: "After the successful first event in Beijing last June, we were delighted to host the second round of our Global 5G Series in Rome. This conference in Rome with sessions on the hot topics of 5G gathered experts from the five organisations involved and enabled fruitful presentations and debates. Participants discovered the latest results and demos from 17 5G PPP projects. This event has also strengthened the collaboration on 5G research and development between our organisations."

The next event in the series of Global 5G events will be held in Tokyo on 24-25 May 2017.

Further information on the programme and the conference, including most of the presented slides, can be found at https://5g-ppp.eu/event/second-global-5g-event-on-9-10-november-2016-in-rome-italy/

News in brief

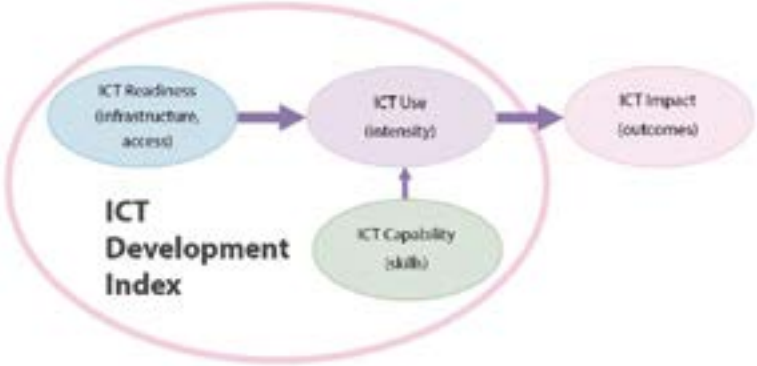
Korea tops the ICT development index

The world is getting more and more connected, according to ITU's annual "Measuring the Information Society Report", which was published in November 2016. However, despite almost ubiquitous network coverage, over half of the world population have not joined the connected world yet.

At the end of 2016, there are almost as many mobile-cellular subscriptions as people on Earth, and 95% of the global population lives in an area that is covered by a mobile-cellular signal. However, as many people have multiple subscriptions or devices, this figure does not provide the whole picture.

The spread of 3G and 4G networks across the world makes the Internet increasingly available to more and more people. In 2016, mobile-broadband networks covered 84% of the world's population. However, with 47.1 % Internet user penetration, the number of Internet users remains well below the number of people with network access.

Huge differences between countries and regions in regard to the ICT Development Index (IDI) remain. The Republic of Korea tops the IDI rankings in 2016 for the second consecutive year. The top 10 countries of the IDI 2016 also include two other economies in the Asia-Pacific region, and seven European countries. Europe continues to lead the regional comparison in ICT development. It had the highest average IDI value among world regions (7.35). On the other end of the scale, the average IDI 2016 value for the Africa region was 2.48 points, just over half the global average of 4.94.



Three stages in the evolution towards an information society (Source: ITU, Measuring the Information Society Report 2016, p. 8)

Three island countries in the Caribbean – St. Kitts and Nevis, Dominica, and Grenada – featured among the most dynamic countries with strong improvements in their IDI value and rank.

http://www.itu.int/en/mediacentre/Pages/2016-PR53.aspx

Record number of patent applications from China

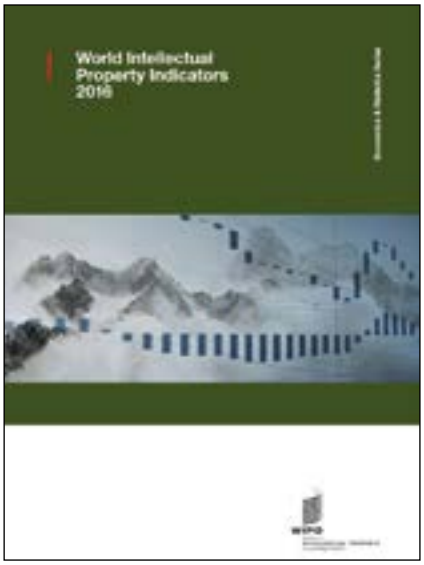
Innovators in China pushed global patent applications to a new record in 2015, filing more than a million applications for the first time ever within a single year.

In total, innovators around the world made some 2.9 million patent applications in 2015, representing a 7.8 % increase over 2014 and the sixth straight year of rising demand for patent protection, according to the annual World Intellectual Property Indicators (WIPI) report by WIPO, the World Intellectual Property.

While Chinese innovators filed the most patent applications (1,010,406) in 2015, followed by those from the United States of America (526,296) and Japan (454,285), they are comparatively home-focused: Innovators based in China filed 42,154 applications for patents outside their own borders, while U.S.-based innovators were the most outward-looking, with 237,961 patent applications filed abroad.

Global industrial design applications filed in 2015 grew by 2.3 %, rebounding from a sharp decrease recorded in 2014 when there was a large drop-off in filings in China. Designers across the world filed 872,800 applications containing 1.1 million designs. Growth was mainly due to increases in applications filed in China, the Republic of Korea and the U.S.

http://www.wipo.int/pressroom/en/articles/2016/article_0017.html



Ericsson forecast: 5G subscriptions to reach half a billion in 2022

The Swedish telecoms equipment provider Ericsson forecasts that there will be 550 million 5G subscriptions in 2022. According to the November 2016 edition of the Ericsson Mobility Report, North America will lead the way in uptake of 5G subscriptions, with 25 % of all mobile subscriptions in this region predicted to be for 5G in 2022.

Asia Pacific will be the second-fastest growing region for 5G subscriptions, with 10 % of all subscriptions being 5G in 2022. Ericsson expects Middle East and Africa to dramatically shift from a region with a majority of GSM/EDGE-only subscriptions, to 80 percent of all subscriptions on WCDMA/HSPA and LTE in the timeframe 2016 to 2022.

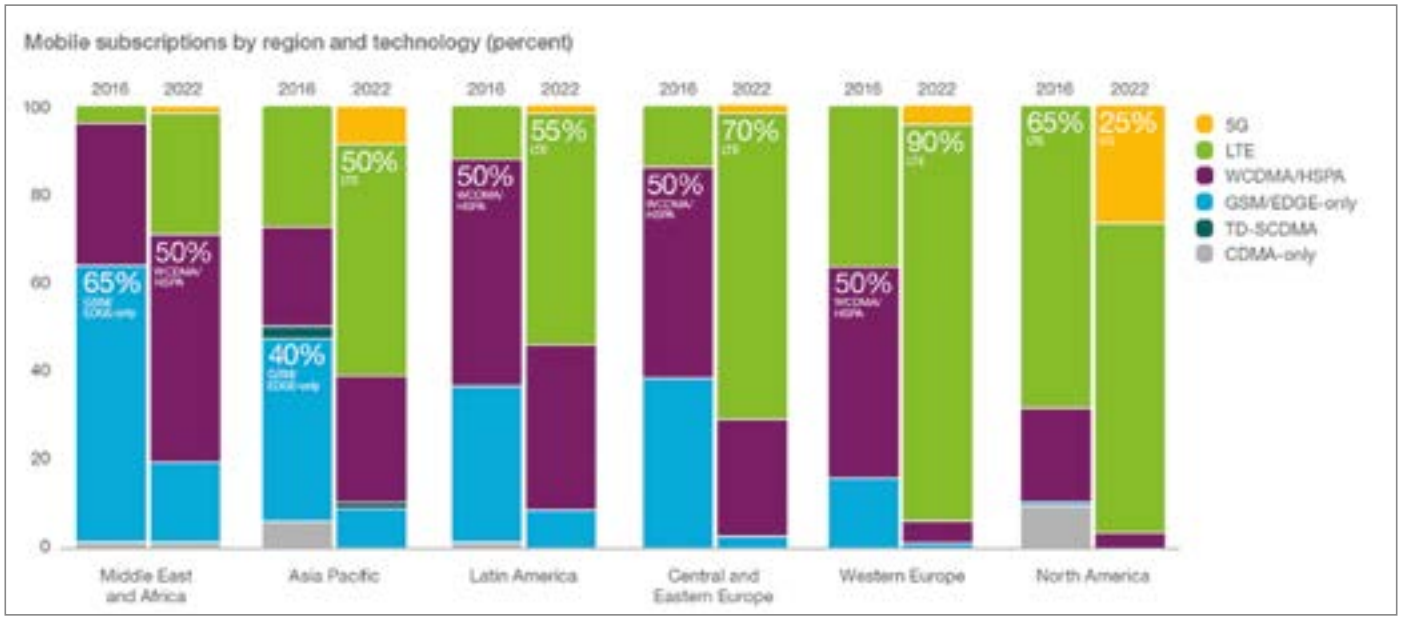
By the end of 2016, there will be 3.9 billion smartphone subscriptions. Almost 90 percent of these subscriptions will be registered on WCDMA/HSPA and LTE networks. By 2022, the number of smartphone subscriptions is forecast to reach 6.8 billion, with more than 95 % of the subscriptions registered on WCDMA/HSPA, LTE and 5G networks.

The report also forecasts that in 2022, there will be 8.9 billion mobile subscriptions, of which 90 % will be for mobile broadband. At this point in time, there will be 6.1 billion unique subscribers.

As of the third quarter of 2016, 84 million new mobile subscriptions were added during the quarter to reach a total of 7.5 billion, growing at around 3 % year-on-year. India grew the most in terms of net additions during the quarter (+15 million), followed by China (+14 million), Indonesia (+6 million), Myanmar (+4 million) and the Philippines (+4 million). Mobile broadband subscriptions are growing by around 25 percent year-on-year, increasing by approximately 190 million in Q3 2016 alone. The total number of mobile broadband subscriptions is now around 4.1 billion.

Mobile data traffic continues to grow, driven both by increased smartphone subscriptions and a continued increase in average data volume per subscription, fueled primarily by more viewing of video content. In Q3 2016, data traffic grew around 10 % quarter-on-quarter and 50 % year-on-year.

https://www.ericsson.com/thecompany/press/releases/2016/11/2056743



A nightmare on IoT street

Things you should know about the Internet of Things

Milon Gupta
Eurescom
gupta@eurescom.eu

The Internet of Things holds the promise of a brighter future. In the smart IoT world of connected devices, your smart thermostat will provide exactly the room temperature you like when you get up, your smart fridge will have ordered exactly what you need for breakfast, your front door will lock itself automatically when you leave, and your autonomous car will safely drive you to work. So much about the bright side of IoT street. Let us now look at the dark side.

Here is the nightmare version of your day on IoT street: After you entered your autonomous car, it suddenly decides that it doesn't want to go to work, but rather have a car wash in the next pond. After you have managed to get out of your car and found a taxi to take you home, despite your wet clothes, you notice that the automatically locked front door is now open. Hackers had opened it remotely and carried away all your articles of value while you were away. They knew exactly where to look, because they had hacked into the cameras that you had installed last summer to monitor your home remotely from your vacation resort.

Your day is ruined and you go to the fridge to get a beer. What you don't know is that your smart fridge has been turned into a zombie. As one of millions of zombie devices in a botnet, it is happily taking part in spam attacks while you are enjoying your beer.

Not so good vibes

If you are thinking now that this story is a bit farfetched, be assured that most of the described hacks have already been done, and the vulnerabilities of smart connected devices really exist. In fact, with smart apps and devices having become ubiquitous, even more intimate violations of data security and privacy have happened.

In May 2016, a woman from the Chicago area bought a We-Vibe Rave self-massage device from a local retailer and later downloaded the companion We-Connect app. She used the device several times. What she did not know: each time she turned on the app, the company was monitoring her activities and collected personally identifiable information – at least this is what she claims in the lawsuit. The woman is suing Standard Innovation, the Canadian manufacturer of We-Vibe, claiming the smartphone-enabled personal massager secretly transmitted "highly intimate and sensitive data" of her usage to the company in real time.

The smart unsafe home

In the IoT world, any connected device or application is potentially vulnerable. While most users are protecting their personal computers against hackers, doing this for connected devices like refrigerators and other household devices is rarely done. Apart from unaware users, this is not supported and facilitated by most manufacturers. Building in security and privacy by design is a cost and undermines competitiveness in price-sensitive markets.

Thus, there are many connected household devices that provide easy access to hackers. According to a Wired report from May 2015, baby monitors are "crazy easy to hack". The report quotes a test by security firm Rapid 7 according to which eight of nine internet-connected baby monitors had serious security vulnerabilities.

And it does not end with this. There are also smart lightbulbs with vulnerabilities that allow cyber attackers to gain access to the home network and smart plugs that can be controlled by anyone who knows their MAC address.

How to make IoT street safe

In order to avoid a surge of nightmares on IoT street, a lot of things have to happen to make the Internet of Things safe. On a technical level, the development of standards and regulatory requirements needs to be progressed in order to make solutions like the ones developed in the RERUM research project (see article in this issue) mandatory.

In addition, users need to act responsibly in order to protect their data. If you adhere to the following three recommendations, you will already significantly reduce your risk:

Firstly, buy devices with a high standard of security and data privacy. Check the data privacy policy of the producer/provider of a product/service. Data privacy issues of providers can quickly turn into security nightmares, when your data are hacked on the provider's server, as has happened to millions of users in recent years.

Secondly, apply the same security procedures like for protecting your PC. This includes having hard-to-crack passwords and changing them now and then. Furthermore, update your devices instantly to make sure you do not allow hackers to exploit the weaknesses of a vulnerable firmware version.

And thirdly, make sure your home network is well protected. This includes, for example, setting up a different SSID for all of your smart devices in your home router. In case one of your devices is hacked, the intrusion will be limited and will not affect your whole home network.

It is up to regulators, industry and users, whether IoT will turn into a dream come true or a nightmare.

EuresTools

The Top Choice for Horizon 2020

Effective Tools for Successful Projects

EuresTools is a comprehensive suite of Cloud-based software tools which facilitate controlling and reporting and enable project teams to communicate and manage information effectively. Over 200 successful European research projects and initiatives have already benefited from **EuresTools**.

Contact us at **services@eurescom.eu** to get further information.

http://www.eurescom.eu/EuresTools

EURESCOM

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

Innovation through Collaboration

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

QR code to the online edition of Eurescom message