FITCE Forum

www.fitce.org Newsletter of Federation of Telecommunications Engineers of the European Union March 2014.

Successful Congress in Leuven….
….next Naples Italy.

Naples FITCE 2014: CALL FOR PAPERS.

Message from Our President

Dear FITCE Members and Friends,

Please let me turn your attention to the actions we've took up till now, following the decisions of last Comité de Direction meeting in Madrid (November 2013). This 251st CD meeting was in particular importance, because of in depth discussion of the Special Report on "A Future for FITCE" prepared by the ad-hoc committee established at the previous CD in Leuven. The members of the committee, namely George Agapiou (GR), Maria Nuño (ES), Andrea Penza (IT) and Andy Valdar (chair, UK), with the support from Jos Gerrese, previous President of FITCE, Maurizio Mayer and Mauro Ugolini (IT), Susanne Blaha (AT), Wim van der Bijl (NE) and José Van Ooteghem (BE), have structured the report around the characteristics of future FITCE, a suggested model of future FITCE and a time line of the transition to the new FITCE 2015.

Wojciech Halka
FITCE President

Following this time line, detail specification of constitutional changes have been prepared by the end of March 2014. This month National Associations will be asked to provide final comments (till the end of April) and they should be approved by next 252nd CD in Rome on 9th May. So, by mid June the proposals will be delivered to the members of General Assembly and in September, during the FITCE GA meeting in Naples, proposed changes are expected to be approved. The implementation of new regulations and new model of FITCE will start just after the Congress in Naples. Having in mind the main characteristics of future FITCE, i.e. central role of the organisation within Europe, strengthening of the congresses, new concept of membership and value chain for members, and low administrative costs, the importance of proposed transformation of FITCE should be clearly seen by all of our Members and National Associations, so we do expect wide acceptance of proposed changes and strong support for their implementation.

As it was already announced, the 53rd FITCE Congress will take place in Naples from 10th to 13th of September. This famous and beautiful Italian city will host our Congress at the "Federico II" University Congress Centre.

(Continued on page 2)

Report from Leuven FITCE 2013.

FITCE 2013 in Leuven proved to be one of the most successful FITCE Congresses in recent years mainly because FITCE Belgium partnered with a number of distinguished Belgian Companies in the security domain such as b-ccentre, I-Minds, ICRI and KU Leuven, the Catholic University of Leuven in organising the Congress. There were 201 Delegates, 46 Speakers and 27 Partners in all which was a delegate number not seen for many years at a FITCE Congress.

The location of the Congress, within the very historic

Congress Hall leuven

University City of Leuven was an excellent choice and facilitated a learning environment which resulted in

Contents.

(Continued on page 2)

(Continued from page 1)

FITCE Italy (AICT), the organiser of the Congress, together with FITCE Greece and FITCE Spain, under their regional Mediterranean initiative, have proposed an interesting subject "From Network Infrastructure to Network Fabric: Revolution at the Edges". It covers interesting issues of new and converged networks and technologies: Smart Cities, Internet of Things, Software Defined Networks etc. For all details please refer to the Call for Papers and our website. In line with FITCE Congress tradition an interesting social programme is also proposed, maintaining friendly fellowship contacts between our Members and their families. I am sure there is no further need to provide greater attraction to your coming to this years Congress!

Let me finish with one more appeal: we all are looking for more information from your National Associations and your local activities. Please send us messages about the main telecommunication, IT and electronic media events in your countries. This exchange of information is very important for Members of our Federation. We are looking for the experience of each of our Association to profit the exchange of professional knowledge and practise throughout Europe, for the benefit of our Members.

See you soon at this years Congress in Naples.

Wojciech Hałka
President of FITCE.

(Continued from page 1)

plenty of Networking between delegates.

Delegates at the Leuven Town Hall.

The Theme of the 52nd FITCE Congress "Moving towards Trustworthy Digital Ecosystems", was very topical and attracted many high quality speakers from the worldwide Cyber-security Industry.

Before the official Congress there was a gathering of delegates at the Leuven Town Hall where delegates were addressed by the Deputy Lord Mayor of Leuven.

The Conference opened formally on Thursday 5th Sept with 2 keynote speeches from key individuals in the Cyber Security Industry in Belgium and 2 Keynote speeches from external speakers. An overview of these keynotes and all other presentations is covered in the section "Congress– Summary of Key Issues".

Delegates enjoying lunch.

The Congress was also addressed by Video message from Neelie Kroes, Vice-President of the European Commission. Her goal is to have a common set of Cybersecurity capabilities for each nation state. The Congress was very significant in that it contained stakeholders of the Cyber-security Industry from all sections including Government Ministries of Security, Cyber Crime Operations Units from many different Police forces, Cyberstrategy experts from major Telecoms Companies and equipment providers, Cyberstrategy strategists from within the Banking Industry, Cyberstrategy Research experts from many Universities, Policy makers from within the European Commission DG of home affairs, and last but not least Cybersecurity Centres of excellence. All this led to a very wide and up to date view of the current Cybersecurity Space, and a very honest look at the very real complexities and challenges.

The quality of the Presentations and Keynote speeches was very high and there was a live twitter feed available

Delegates visiting the Fitce Belgium Room.

for the Congress Participants to view at the side of the main stage. During the Congress Fitce Belgium provided a separate room for all delegates to meet and network, and enjoy some light refreshments.

Many thanks are due to the Organising Committee including Prof Jos Dumortier, Nicole Verbiest , Marc Verbruggen, Walter Van Hemeledonck, Georges Devroey, Gerard De Catelle and the team of red-shirted young people, who were always present to ensure the Congress ran smoothly.

The Conference closed on Friday afternoon with a closing keynote entitled "Towards Achieving Cyber Resilience in EU and Beyond", by Heli Tiirmaa-Klaar, the Cyber Security Policy Advisor at European External Action Service.

Saturday morning was for Fitce members and the Fitce General Assembly was held. This was chaired by Jos Gerrese the outgoing President. One significant contribution was from Andy Valdar from FITCE UK who gave a strategy presentation on the future of Fitce. This is viewed as highly critical to where Fitce will be heading over the next year or two, and presents a number of options including a sunset strategy. It was then time for the new Board of Officers to be nominated and confirmed. Our temporary Secretary General, Walter Van Hemeledonck of FITCE Belgium was confirmed as the new Secretary General. Georges Devroey continued as the Treasurer. Our New President Wojciech Halka from FITCE Poland was appointed in absentia. Our outgoing President Jos Gerrese handed over the FITCE Chain to the new Vice President Maurizio Mayer of FITCE Italy. A second Vice President Mauro Ugolini of FITCE Italy was also appointed.

FITCE General Assembly.

Great tribute was paid to Jos Gerrese for his inspirational leadership of Fitce during the last 2 years.

Looking to Naples Italy.
FITCE 2014.
53rd FITCE Congress.
"From Network Infrastructures to Network Fabric: Revolution at the Edges".
10th to 13th September 2014.

The Conference.

Fitce Italy are pleased to announce that FITCE 2014 will beheld in Naples, under the auspices of AICT with the support of FITCE Greece and FITCE Spain, which constitute the Euro Med Telco Forum.

Maurizio Mayer.
Congress Chair.

Euro Med Telco Conference 2014 is at the same time the 53rd edition of the annual Fitce International Congress and the first open event organized by the Euro Med Telco Forum (EMTF).

Fitce is the well known Federation of the Telecommunications Engineers of the European Union while EMTF is a platform founded by the Greek, Italian and Spanish Fitce branches that aims to extend the ICT cultural activities beyond the European boundaries to reach all the Mediterranean area. The Naples choice for this first edition wants to be a clear geographical sign in this direction.

We believe that a strong contribution to the economical and social progress of this wide area may come from the recent advances and wide distribution of the latest ICT researches and related applications. For this reason we have chosen a subject for the scientific and technical sessions in line with the most recent developments and market trends.

Beside the technical program we will have round tables regarding interesting topics related to the diffusion of these techniques, like: Do we need a Digital Agenda for the Mediterranean?

We therefore invite all the ICT community in and outside the Euro Mediterranean area to contribute and participate to this new initiative.

The Subject

In these last few years we have seen a growth in the local networks, wifi, bluetooth, sensors' networks. We have also seen several constituencies setting up their local networks, like in malls, airports. Some of these are actually city wide, set up by Municipalities.

In the coming years we are going to see further deployment of these networks as well as of halo nets created by terminals themselves, like a cell phone creating a local network that can be used by a variety of devices to connect to the big infrastructure and with one another.

This is leading to a revolution at the edges, supporting the connectivity at ambient level and decoupling the end user from the main infrastructure. Actually, we are also seeing double SIM cell phones that can connect to two Operators networks and the advent of the Soft SIM is likely to multiply the access option for a terminal.

All of this tells us that we are moving in terms of the end user from a single Network Infrastructure to a Network Fabric. Clearly this has significant implication for the Operators that by 2015 in Europe will find their own market space populated by all other European Cell Phone Operators: an increase in connectivity options from a few to over a hundred!

This connectivity fabric will also provide major opportunities to many partners making the Internet of Things more and more feasible.

The Topics.

This Event particularly invites presentation of novel work and experiences in the following areas:

- Smart Cities: ensuring seamless connectivity.
- IoT: connecting things and sensors for ambient awareness.
- Open data framework: leveraging data from the networks.
- Services and application leveraging a pervasive network fabric.
- SDN across network domains, technology, policies and business models.
- The challenge of zero cost connectivity.

The Programme.

The following is an outline of the delegate programme, which will have technical Sessions on Thursday and Friday.

Wednesday 10-9-2014

15.00-19.00 Registration open

19.30-21.00 Welcome reception

Thursday 11-9-2014

9.30-13.00 Opening session

13.00-14.30 Lunch

14.30-18.00 Technical sessions

Friday 12-9-2014

9.30-13.00 Technical sessions

13.00-14.30 Lunch

14.30-18.00 Technical sessions

21.00-24.00 Gala Dinner

Saturday 13-9-2014

10.00-11.30 FITCE General Assembly

11.30-13.00 Congress Conclusions.

There will also be an interesting Partner Program, the main two events being,

- A Visit to the city of Naples by Bus and foot.
- A visit to the Island of Capri (tbc).

On behalf of Fitce Italy and the EMTF, I look forward to meeting you in Naples. Updates on the progress of the Congress will be available on the Congress Website and also on the FITCE Website.

A Call for Papers has already been issued.

Kind Regards,

Maurizio Mayer,

Congress Chair.

Call for Papers.

MED TELCO EURO forum

Euro Med Telco Conference 2014

FITCE 53rd FITCE International Congress

Naples (Italy) 2014. September 10th to 13th. University of Naples. Federico II Congress Centre.

From Network Infrastructures to Network Fabric: revolution at the edges

In these last few years we have seen a growth in the local networks, wifi, bluetooth, sensors' networks. We have also seen several constituencies setting up their local networks, like in malls, airports. Some of these are ac- tually city wide, set up by Municipalities.

In the coming years we are going to see further deployment of these networks as well as of halo nets created by terminals themselves, like a cell phone creat- ing a local network that can be used by a variety of devices to connect to the big infrastructure and with one another.

This is leading to a revolution at the edges, supporting the connectivity at am- bient level and decoupling the end user from the main infrastructure. Actually, we are also seeing double SIM cell phones that can connect to two Operators networks and the advent of the Soft SIM is likely to multiply the access option for a terminal.

All of this tells us that we are moving in terms of the end user from a single Net- work Infrastructure to a Network Fabric. Clearly this has significant implication for the Operators that by 2015 in Europe will find their own market space pop- ulated by all other European Cell Phone Operators: an increase in connectivity op- tions from a few to over a hundred!

This connectivity fabric will also provide major opportunities to many partners making the Internet of Things more and more feasible.

This Event particularly invites presentation of novel work and experiences in the following areas:

- Smart Cities: ensuring seamless connectivity.
- IoT: connecting things and sensors for ambient awareness.
- Open data framework: leveraging data from the networks.
- Services and application leveraging a pervasive network fabric.
- SDN across network domains, technology, policies and business models.

Authors are invited to submit high quality papers (in English) reporting original research results and field experiences related to new network deployment and innovative services on the indicated topics.

The peer review process will be based on Full Papers. They must be submitted in PDF at the EDAS page exclusively (http://edas.info/newPaper.php?c=17527). Accepted camera-ready papers will be in PDF and formatted in the standard IEEE double-column conference template that may be downloaded here. Maximum 6 pages are allowed for each paper, including all figures and references.

The paper shall be sent no later than May 15th 2014 through EDAS.

Authors will be notified of their contribution acceptance by July 31st 2014 and will submit the final camera- ready papers within August 15th 2014.

A copyright and consent form, which transfers to AEIT-AICT all rights under copyright concerning the paper, must be endorsed.

Each accepted paper must have an oral presentation at the Conference by one of the authors that have paid a full quote. In case of multiple papers an author will be allowed to present maximum 2 papers for a single full quote paid.

The accepted and oral presented papers will be published in the Conference CD-ROM distributed to all participants.

IMPORTANT DATES
Contributions Submission Deadline:
May 15th, 2014
Notification of Acceptance:
July 31st, 2014
Camera-ready papers submission:
August 15th, 2014

EDAS link:
http://edas.info/newPaper.php?c=17527

organized by AEIT Associazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telecomunicazioni; AICT Società AEIT per la Tecnologia dell'Informazione e delle Comunicazioni; DIETI UNINA

with the support of FITCE Hellenic Union of Telecommunications Engineers; Hellenic Branch of FITCE

General Chair: Maurizio Mayer, AEIT-AICT

Scientific Committee Chairman: Luigi Paura, University of Naples Federico II

Scientific Committee Co-Chairmen: Wim Van Der Bijl, Cap Gemini - FITCE Francesco Vatalaro, University of Rome Tor Vergata.

Leuven Congress Highlights

Congress Day 1.

The Congress started with 4 high level keynote Presentations. The first was "Securing Cyber Space in Belgium", by Luc Beirens, Head of the Belgian Federal Computer Crime Unit (FCCU).

He presented an overview of the Belgian Network Information Security Organisation BELNIS whose main goal is to produce a Cyber Security Strategy (CSS) for Belgium. He also pointed out that current international agreements are not sufficient to protect Belgium when a Cyber incident hits the country. His goal is to have a Centre for Cyber Security in Belgium.

The second keynote was "A Belgian Good Governance Guide for Cybersecurity", by Rudi Thomaes, Secretary General International Chamber of Commerce Belgium.

Part of Congress Audience.

He spoke about the development of Belgium Cyber Security Guide in co-operation with Microsoft and Ernst & Young which will have 10 main principles and 10 main actions that will be usable by any Company. He indicated a 40% increase in Cyber Crime in 2012. Also 35% of Companies do not have a threat intelligence initiative.

The third keynote was "Self evolving defences against self-evolving malware", by Yvo Desmedt, Jonsson Distinguished Professor at the Department of Computer Science of the University of Texas at Dallas.

The last keynote was "Anonymous And The Future Of Hacktivism", by Parmy Olson, Forbes (San Francisco) journalist and author of the recent bestselling book

Parmy Olsen presenting at Congress.

"We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency" (2012).

She pointed out that recent evolution of Syrian Electronic Army as cyber warfare against US interests indicates the speed of cyber terrorism. The ultimate goal is the embarrassment of others. Anonymous became a force for international activism through digital protest by attacking websites. Lulzsec evolved from a group of 6 high level hackers who left Anonymous. It has since split up. Habij is a tool used to organise SQL attacks on databases. Tools such as Andrat are available to break into smartphones. Her talk was all the more interesting in that it gave a very good insight into the mind of the hacker and the alter-persona taken on during hacking activities and interaction with other hackers.

National Cyber Security Strategies.

The next Session explored "National Cyber Security Strategies" where speakers from Australia, U.S. and the Netherlands presented their national cyber security strategies, that are worldwide considered as the "best practice" in the field.

In Australia the journey of CS Strategy (CSS) started in about 2004. 700 CS incidents were reported in 2012 twice the level of 2011. The 3 stakeholders are Government, Industry and Community. Cyber Emergency Response Teams have been established all over Australia with a CS Centre to co-ordinate all interests.

In the US the first CS Strategy was developed in 2003. In 2008 a comprehensive national Cybersecurity initiative was undertaken and in 2010 a Cyberspace Policy review was initiated by the Obama Presidency. There is a balanced approach which includes focus on economic and social issues as well as the security threat issues.

In the Netherlands, the first CS Strategy was released in

(Continued on page 6)

Report from FITCE Greece International Workshop. Athens September 2013.

Great success at the International Workshop on NGAs in Athens.

Athens Workshop

On Wednesday 10/09/2013 an international workshop was organized at OTE (Greek incumbent telecom operator) premises. It was quite successful with very interesting

(Continued on page 7)

2011. It is an umbrella strategy and action program with a public/private partnership. In the discussion afterwards, maintaining confidence in the program, continually participating in the process and keeping technically up to date were mentioned as the biggest challenges for strategy implementation.

The next Keynote session was a presentation on "Cyber Westphalia", by Chris C. Demchak, Professor at Strategic Research Department at the Center for Cyber Conflict Studies (C3S), United States Naval War College. He indicated that Cyberspace is a globally open and easily abused substrate. Scale, Proximity, and Precision are 3 characteristics that cyber-conflict possesses. Top 6 Corps in US have spent $230 billion in 2010 alone on CS (2011 Poneman Institute Study).

The next keynote session was "Readiness And Resiliency: Developing National Cybersecurity Strategy", by Paul Nicholas, Senior Director, Trustworthy Computing at Microsoft. He spoke about Global technology trends. One of the significant predictions is that 75% of data in the next 5 years will be in someone else's control. In addition global discussion in Cyber Security should be the norm for any nation state.

International Cyber Security Cooperation.
Speakers from the U.S., Europe and Australia presented their view on cyber security cooperation at the global level. There is US - EU agreement on tackling Cybercrime The Australian Federal Police gave an example of the complexity on international cybercrime where 500,000 credit cards in Australia were compromised by a gang in Romania. In Europe a European Cyber Crime Centre has been established by Interpol, but nonetheless there is a large dependence on Financial Institutions and ISPs to release data to assist. Also 3rd world countries can do alot of damage to EU without ever leaving country. There are no Cybercrime agreements with China, Africa, or South America.

Threats and Challenges in the Smartphone Era.
Four speakers presented their view on threats and security challenges with mobile devices. Some of the interesting points made were,

- The huge penetration of mobiles e.g. 7 billion mobiles in both China, India and APAC.
- A need for Security via strong PIN, Anti-malware software and only using trusted sites.
- The need for a 3 fold technology approach- secure hardware components, on device encryption/virtualisation, and biometric user authentication with 3D face recognition.

Congress Day 2.

The 2nd Day of the Congress opened up with a video message from Neelie Kroes, Vice-President of the European Commission. In her talk she mentioned that the EU was not prepared for Cyber Security implications and that it needs to be addressed with the respect it deserves. Her ideal is to have a common set of Cybersecurity capabilities for each nation state.

The second Keynote dealt with "Safety on the internet", by Saskia Van Uffelen, Digital Champion Belgium, CEO Belux Bull and CSB Consulting. He indicated a predominant attitude of….let's hope we don't have a CS disaster before we are able to deal with it. He raised the question of whether or not companies have an online security policy?

The next keynote was "What is a seven-year view anyway?", by Ross Anderson, Professor of Security Engineering at Cambridge University, England. He indicated that the complexity of real world systems was the killer and that in the next 5 to 7 years data protection will break.

The third keynote was "Credit Card Fraud: Criminal Models, Actors and Money Laundering", by Mauro Vignati, Senior advisor at MELANI. He gave a few case studies of recent cases of stealing of credit card data. One was where, using JavaScript injection into Facebook credit card information was stolen. He also described the process of

Congress Panel Discussion.

getting goods bought by stolen card from US to Russia, primarily by printing duplicate postal labels to mules to send goods to final destination.

Hit by a Cyber Attack: What Did We Learn?
This session was based on the lessons learned by Cyber attacks. In one case hackers got into a major Telecom Operators customer database through a vulnerability in backup software. It took 10 days to fix the problem, but only 2 days for social media to get the story. Communication within the organisation was slow initially. The lessons learned were (1) don't destroy the evidence before applying the fix, (2) have Asset Management System up to date and (3) know the Stakeholders.

In another case a Bank was made vulnerable through DDoS attacks lead to unavailability of online banking systems. Social Media got on the case quickly and many incidents of Phishing arose on the back of the DDoS attack. In this case early communication with Customers was important to manage the Customer mindset.

Afternoon Keynote Sessions.
The first afternoon keynote session was "Security Battle-

Part of the Congress Team.

ground", by Brian Kenyon, Vice President & Chief Technology Officer of Security Connected, McAfee. He had a number of key strategic points for Companies, (1) Simplifica-

(Continued from page 6)

tion of Security for non-tech managers, (2) One size fits all security does not work, (3) The cost of proactive breach analysis is 50% the cost of reactive breach, (4) Top down hacker-mindset approach is essential.

The second afternoon keynote session was "Some Assembly Required: Implementing Cyber Security Strategies in the 21st Century", by Noshir Contractor, Professor of Industrial Engineering and Management Sciences, Northwestern University, Chicago, U.S. He outlined how to assemble teams for CS Strategy and also presented some of the algorithms that best gets teams together.

There were then 2 lively Panel Discussion, the first on "Enterprise Information Security Governance: Why Do You Need It?" and the second on "Creating Trustworthy Digital Ecosystems: How Do You Do It?" Both sessions, despite being at the end of the Congress, managed to get lively discussions going with plenty of audience questions.

The closing keynote of the Congress was "Towards Achieving Cyber Resilience in EU and Beyond", by Heli Tiirmaa-Klaar, Cyber Security Policy Advisor at European External Action Service. She outlined a number of important points, (1) EU CSS does not all come from Brussels and are led from EU Capitals, (2) Not all capitals are set up to do CSS property, (3) The Public Sector lags behind the Private Sector, in CS, (4) Proper CSS requires Public Private partnerships and (5) it is difficult to deal with cost of CS breaches coming from countries that have no CSS framework.

The Congress ended on a high note and proved to be a very successful Congress with some attendees stating that it was the best Cyber Security Conference they have attended, and included a very wide variety on presentations from a very complete list of stakeholders in the Cyber Security Industry. Great credit is due to the Organisers, all of whom are associated with Fitce Belgium.

All Congress Presentations are available to download from the FITCE Website http://www.fitce.org

(Continued from page 5)

talks by 10 top quality speakers from industry/ academia and over 120 participants. It is worth noting that the event was also attended by the Vice President

Workshop Audience.

of EETT (Greek Telecom Regulator), the president of FITCE Greece, as well as executives from the fixed & mobile telecom industry (from Greece and abroad) and academics from several Greek Universities.

The workshop presentation and discussions focused on the very interesting topic of "Wireline next generation network technologies in support of future requirements of fixed and mobile users". The great success of the event was warranted by the presence among the speakers of scientists with worldwide reputation like Prof. Josep Prat from University Polytechnic of Catalonia, Prof. Ernesto Ciaramella from University of Pisa, and Prof. Ioannis Tomkos from Athens Information Technology Center, who are experts in optical network technologies. Presentations were also given by executives of telecom companies (e.g. Ericsson, OTE, COSMOTE, OPTRONICS TECHNOLOGIES) who have great experience in developing relevant NGA infrastructures. The topics presented include all developments in access networks like: FTTH, FTTSite, Small Cells, WDM-PONs and VDSL Vectoring.

The workshop was organized by OTE and OPTRONICS TECHNOLOGIES under the auspices of the European research project COCONUT (www.ict-coconut.eu) and the National Research Programme PANDA, in cooperation with FITCE. The objectives of the hosting research projects (which involve in their consortia leading companies and universities / research centers such as: BT, Ericsson, OTE, Intracom, Barcelona University, University of Pisa, AIT, Promax, Optronics Technologies, InAccess, NTUA , University of Patras, etc.) is the development of new wireline access network technologies (FTTx – Fiber to thehome / building / cabinet / antenna) that will serve the need for improved access speed and quality of service/quality of experience by the end users, while simplifying the opera-

Workshop Presentation.

tion of the network and ensuring lower operating costs. The purpose of the workshop was the dissemination of results about the latest technology developments to the executives of the telecommunications market in Greece, the related government agencies and to the members of the academic community.

At the end of the workshop, the attendees had the opportunity to watch demonstrations by OPTRONICS TECHNOLOGIES of a live video transmission system using fiber optic passive subscriber access technologies (GPON operating at 2.5Gbps).

Those interested in more details, can find the workshop presentations and photos at the event web-page that is hosted at the web-site of EU research project COCONUT: http://ict-coconut.eu/index.php/news/34-latest-news/52-international-workshop

Presentation from Congress.

Telecom Security in the era of explosive Smartphone growth….. Who cares!

Huib Ekkelenkamp
Atos, Papendorpsweg 93, 3528 BJ Utrecht,
The Netherlands huib.ekkelenkamp@atos.net

1. INTRODUCTION

Gerardus Mercator (1512 – 1594) who studied in Europe at Leuven University gave the world smart maps for improved positioning and travelling. His pragmatic approach to mapmaking, geography and information handling lead to a new orientation on the world; it changed our relations and way of communication.

Mercator changed orientation for faster recognition

Apple and Google gave the world smartphones and mobile operating systems for improved communication and information retrieval. It also resulted for Telcos in a new orientation, including the way of service provisioning, customer care and billing. With the enabling mobile networks it revolutionised the telecommunication and IT world.

The change from voice to text, graphical and video communication was enabled but also stimulated by the new user interfaces, screens and applications. Wiping, tapping, and changing the orientation of the screen of a mobile device resulted in a different way of communication. Video, pictures, graphics, icons, avatars, and widgets have changed the user interface and increased the transported data volume considerable.

A wide range of services and content is provided by numerous parties, including Telcos (telecom operators), businesses, banks, governments as well as end-users. Over-The-Top (OTT) service providers use the Telco infrastructure without owning and managing the network. With so many parties involved this leads to security issues. Confidential and privacy information, including financial transactions, medical data, business strategies, industrial and trade secrets, need to be protected against intruders who want to gain benefit or disturb people or organisations. The enlarged use and sophistication of smartphones and tablets increased the security problem. The changing telecom world, described hereafter in section 2, shows a large growth of mobile communication. The main threats and security issues for smartphones, which are presented in section 3, need special precaution. Attacks on the network, the different mobile operating systems and the mobile Apps installed on the smartphone or tablet elaborated in section 4 require also special attention. The potential protection and security solutions for smartphones, described in section 5 will result in improved mobile cyber security. Who cares and provides security guidelines, given in section 6 provide valuable sources for better protection. Conclusions summarised in section 7 give an overview of the main recommendations. Used references in section 8, include also some books, websites on the subject and some Apps for better protection.

2. THE CHANGING WORLD OF TELECOMS WITH SMARTPHONES AND TABLETS.

Telecom development is characterised by major paradigm changes in technology, services and usage. Mobile communication and internet are the changes of the end of the 20th century. However, their combination resulted in the first decennium of the 21st century in another change: broadband mobile access to internet, including

The change from telephone to smartphone is drastic

email, video, transactions, and mobile payments. With further developments in networks, mobile handsets, user interfaces, screens, operating systems, applications, processors, batteries, and sensors a complete new concept emerged: the 'Smartphone' written as one word.

It could be considered as another paradigm change in telecommunication. It enabled all communication and processing in a tiny unit, as a companion wherever you go. It became an irreplaceable tool or gadget in private and business life. Everywhere in the world people are hooked to their smartphone, be it at home, on the move or in the office. No train or most of its passengers read on their screens or type messages. With the smartphone, data dominates voice. With smartphone sales comprising in Europe over 50% of mobile sales, the penetration is growing fast.

The mobile growth is in the Far East

With over 6.5 billion mobiles, and only about 1.2 billion fixed lines worldwide now, wireless communication became in less than 20 years dominant as shown in the next figure. The volume is created in the Far East with China, India and other Asia & Pacific each 1 billion mobiles.

With a current world penetration of 30% (or about 2 billion), smartphones dominate in many countries. The remaining 70% are cheap feature phones which also deal with security issues. These phones are expected largely to be replaced by smartphones in the coming 10 years.

(Continued from page 8)

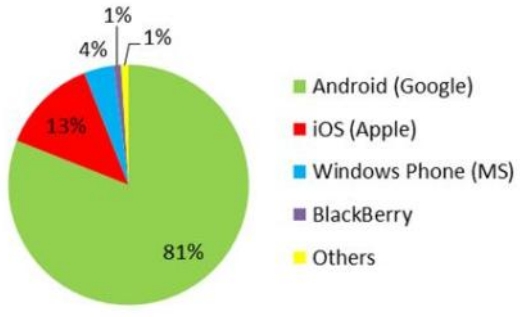
This is stimulated by the rollout of new networks of which the LTE (Long Term Evolution) broadband IP based 4th generation will provide the cheapest solution for large volumes and high traffic.

Machine to Machine (M2M) communication is expected to grow fast as well. The 'internet of things' will connect cars to service stations, remote sensors to data processing units, and detectors to surveillance units so that human interference can be reduced for servicing, monitoring and protection.

The availability of mobile applications or Apps from the App stores, their free provisioning or low price, ease of installation and payment has stimulated the use of smartphones drastically. With over 0.5 million Apps on Apple iOS and Google Android each, the choice is almost unlimited. The smartphone got its larger equivalent in the tablet using the same or similar mobile operating systems and Apps. The tablets rose almost to the level of laptops, replacing them for many tasks. Smartphones and tablets have still less space on their screens and processing power than PCs, including laptops, which result in a larger vulnerability for security attacks. Also the user behaviour is different. Swiping and tapping on the move are actions which take place in a hurry without careful reading of URLs or acceptance criteria. The trust in mobile sites, Apps, or messages is still great; the number of incidents is limited or less known than that with PCs.

The major mobile operating systems and their market share end 2013 in smartphones are shown in the next picture. Android of Google is with about 81% in the lead, as it can be installed on several hardware platforms. Next comes Apple iOS which is always in combination with Apple hardware platforms.

Microsoft Windows Mobile and the later introduced Windows Phone, has still a low market share but is growing fast, also by its choice of Nokia for their smartphones and the takeover of Nokia mobile by Microsoft. BlackBerry had a comeback with their new OS. Other mobile OS (like Linux and Bada) have limited application (less than 1%).



Mobile OS are dominated by Android and iOS

The smartphone sales themselves show another distribution. With a total of about 1.8 billion mobiles sold in 2013, about half of them are smartphones with Samsung 32% and Apple 13%. The remaining 55% is divided between Nokia, Lenovo, LG, Motorola, HTC, BlackBerry, Sony, Huawei and ZTE.

Use of consumer products for business purposes has been increased. This includes the mobile terminals like smartphones and tablets as well as the use of e-mail, social media and software or Apps. Differences in security, often ignored by consumers are enforced by business rules.

Bring Your Own Device (BYOD) is increasingly popular. Consumers require more facilities than basic communication. Social media, taking photos and videos, gaming, texting (SMS, WhatsApp), banking, financial transactions, navigation, and location based information on the move are some examples of services with more private than business use. This means that mobile devices are more selected to support private services than business services. Some of these services support also business use, so it is also in the interest of the business that users are familiar with them and that experimenting and problem solving takes place in private time. The difference between private use and business use tend to disappear. This means that security requirements for business use are also applied to private use. Authentication by strong password, encryption, secure connections, antivirus software, remote wipe of confidential information (in case the mobile is stolen) and back-up facilities are requirements which benefit the user in all cases.

A balance is required between the user-friendliness and the security protection. If the protection is too rigid it might lead to a work-around or use of other mobiles with less protection.

Smartphones and tablets have an inherent security protection by their hardware and operating systems. However, additional measures are required to prevent malware installation and intrusions which are serious threats.

Mobile devices are also used for remote control. An example is remote car management. This can be starting the engine of one's car and pre-heat or pre-cool it before driving. Other available services are navigation, additional information of the environment while driving (e.g. via Wikipedia), parking and payment facilities, audio streaming and (e-mail) text-to-voice. Also remote servicing, including planning a visit to the garage for maintenance is used. Remote stopping and blocking of a stolen vehicle is another facility. This requires extra safety and security for the mobile communication.

Smartphone security is affected by security and availability of the whole communication infrastructure. This includes the mobile terminal, the network with the wireless and fixed connections and its nodes (servers, routers, switches etc.) as well as all used and supporting software.

Mobile terminals can use a removable memory card which needs additional protection by encryption of the contained confidential information. The authentication of the terminal does not give protection for the card.

Most mobile terminals have a removable SIM card. This requires also special safety precautions for misuse of the card (e.g. SIM pin lock). Mobile terminals are used in different ways and environments than fixed terminals. Smartphones and tablets take over functions of laptops and desktops and are used for many tasks for which confidential information is required like buying goods, financial

(Continued from page 9)

transactions and personal information exchange via social networks. Moreover, presence and location information of the user can also be considered as confidential and needs therefore protection. Limited storage capabilities of the mobile terminal might result in more use of on-line storage (in the cloud). The security depends than also on other parties. The availability and retrieval possibilities of on-line storage are part of the mobile cyber security as well.

The main aspects to consider for security are: loss of terminal, malicious applications, malware (viruses, worms, key-logging), used storage, network connections and means of protection.

The user should define or know what his confidential information is and for which protection is required. Already by being aware of the type of information stored, a base for security is created. It is not easy to oversee the consequences of stolen information. But it can be foreseen that authentication data like username and passwords need more protection than general information about the weather or travel destinations.

Mobile terminals tend to come on more unsafe places than fixed terminals. Users will always carry them wherever they go. Even the tablets are carried more frequently than laptops, be it in commuting from home to work or on holiday. They are also more exposed to public as their capabilities in making photos, videos and use for navigation and location finding can draw attention of a large group of bystanders or onlookers. Moreover, in many countries it can be assumed that most people between 12 and 70 have now a smartphone of considerable value which might be a reason for robbery.

It is always recommendable to make regular back-ups of important data. This is more difficult with data of smartphones and tablets. It can be done via a port using a USB stick or a mobile hard disk, but it can also require a connection with a laptop or PC. In some cases the smartphone has no external ports for back-ups and needs this to be done via the network in the cloud or with a PC. Restoring information in the proper format can also be a challenge as limited practice is available. In particular restoration of settings can be a problem after a new version of the mobile operating software has been installed. Also installation of another application for data handling (like text processing, spreadsheet or graphical information) might give restore compatibility problems.

That means that making back-ups of data on a smartphone can be more cumbersome than of data on a PC. In case of a repair or sale of the mobile terminal, personal data needs to be removed. In that case it is advisable to make a complete wipe of the memory, removing installed Apps and restore factory settings.

3. THE MAIN THREATS AND SECURITY ISSUES: SENSITIVE DATA, IDENTITY, AND SERVICE AVAILABILITY.

Not many users of communication systems are interested in security until they themselves are victim of an attack, or are misled resulting in loss of privacy, money or reputation. They assume that the communication system, websites and addresses are sufficient protected against malicious use and trust the operator and service provider. Smartphones are preferred targets of attacks. These attacks misuse the weaknesses that can come from networks and services like GSM, WiFi, Bluetooth and SMS or MMS. Attacks can also exploit software vulnerabilities from the operating system and web browser. Malicious Apps and software, installed on the smartphone can enable attacks and intrusions. The following figure shows some of the channels and services which are potential security threats. With tethering an internet connection can be shared between several terminals. Not shown is a (USB) power socket or a port for a removable memory card. These access facilities make smartphones and tablets more vulnerable than fixed terminals. Malware can enter in several ways. WiFi and Bluetooth are as radio connections themselves vulnerable but also their connection to the fixed network provides access for intruders. The extensive use of Apps and social networks provide additional threats.

Lending a smartphone to another user is also a point of concern. Malware can easily be installed by visiting an infected site or installing a malicious App. MMS and SMS messages can contain malware which the user would not notice. Trusted senders and understandable messages can avoid misuse. Preferably Bluetooth and WiFi should be

Smartphone access has special security risks

used in a (password) protected mode. Free WiFi or Bluetooth connections involve a higher risk.

Three main security aspects are distinguished: data, identity and availability:

Data: smartphones contain much confidential data, like authentication information, private information, sensitive credit card numbers, agenda, contact data, e-mails etc.

Identity: smartphones are customised by the owner, the parameters are attractive for attackers, and they can steal this identity to commit other offenses.

Availability: smartphones can be disturbed or even made useless for their owners by limiting access through attacks and depletion of its resources like battery and memory

The top security issues for smartphones or mobile devices in general are:

- Physical loss
- Data storage security
- Authentication

(Continued from page 10)

- Multiple user support
- Safe browsing
- Secure Operating Systems
- Apps and installed software
- Denial-of-service attack
- Malware, virus, worms, Trojans, spyware
- Phishing
- Cross-Site Request Forgery (CSRF)
- Location information
- Malicious device drivers
- Multifactor authentication

Physical loss is a main threat. The hardware lost might be a few hundred Euro, the data lost, the uncertainty, the time spent for recovery and the frustration are often experienced as a much higher burden.
Data storage security is not only related to physical loss, but also to intrusions and quality and reliability of the phone. If the phone stops working or cannot access its memory anymore, costs for recovery can be high.
Authentication is now based on strong passwords, combining letters, numbers and special characters. This is awkward on a screen keyboard and takes more time than a simple 4 digit PIN or a swipe.
Unlike PCs and laptops, mobile devices have no multi-user support. Once a user entered a mobile device (by a simple 4 digit PIN) all confidential personal and business information can be accessed.

Safe browsing is also an important security protection. This should prevent the hostile world to get grip on the mobile device. Users have limited resources to prevent intruders or malware to take action. Small screens show not always the whole URL, protection software is light because of memory and processor restrictions. Users like to be fast and ignore warnings by a simple swipe. Moreover, mobile devices are often used for private sites where threats can be greater than for business sites.

Secure operating systems should guarantee a safe processing environment for downloaded Apps, but should also provide reliable communication. Processing should have no limitations on making phone calls or result in fast depleting of the battery.

Users select a smartphone or tablet for the possibility to install Apps. These mobile applications may share data of other applications on the unit which makes them vulnerable to malware. Free Apps can also collect marketing data of the user. "Free" means do direct payment to obtain the App. However, advertisements pushed to the user and data retrieved from the user can be seen as compensation. Often for a modest payment (2 to 10 Euro) the user gets an App with increased functionality, no advertisements and sometimes better protection to intruders. From a security point of view a paid App is a better choice.

Vulnerabilities in the operating system and applications are used and exploited by intruders. Botnets (derived from robot and network) are malicious programs with perform actions over the internet which the user does not intend and is not aware of. Botnets also refer to mobiles or computers which have been recruited by malicious software to behave like zombies. They can be used to generate a Denial-Of-Service attack (see hereafter). Though botnets originated in high performance servers and PCs connected to the internet, they become also a threat for smartphones and tablets as larger numbers can be involved.

Ransomware is installed software which blocks parts of the functionality on the device which can be undone by providing information or payment. This can also be pseudo anti-virus software which asks for payment.

(Distributed) Denial-of-Service or (D)DoS attack is an attempt to make a machine or network resource unavailable to its intended users. It could be the result of an attack on the mobile network focussed on a particular smartphone or tablet operating system, hardware version or category of installed Apps. This could block the voice, e-mail, SMS or MMS facilities. A (D)DoS attack on smartphones or network can result in:

- Depletion of resources, such as bandwidth, memory, battery or processor time.
- Disruption of physical network components.
- Disruption of routing information
- Disruption of state information, like unwanted resetting of TCP sessions.
- Obstruction of the telecom network between users so that they can no longer communicate satisfactorily.

Malware (short for malicious software, see also the definition in the next section) is already long known from the PC and laptop world. Developers can use this large experience for smartphones and tablets. Avoiding spreading though SMS and mobile browsers requires special precautions.

Phishing is the activity of attempting to acquire confidential information such as usernames, passwords, and credit card details (and sometimes, indirectly money) disguised in communication as a trustworthy entity. Phishing is a serious threat as mobile users are less critical in opening sites or mail.

Cross-Site Request Forgery is an imitation of a trusted site by a malicious site, trying to get confidential information of the user. Mobile users rely heavily on clicks on links and e-mails and are less critical on the (partly) shown URLs. E-mail spoofing is the creation of email messages with a forged sender address.

Location security deals with privacy. GPS or radio triangulation provides information about the user's location. This combined with other data can reveal much on the behaviour of the mobile user. Location information can also be positively used as an extra service like in navigation or Google latitude.

Device drivers (as for video or Bluetooth) have full access to the OS and should therefore be safe. Installing a non-secure device driver provides a great risk. Downloads should only be from trusted sites.

Multifactor authentication is used to ensure that the authorised mobile is trying to get access to the mobile website by using multiple characteristics of the mobile. Besides the usual credentials also the device signature based on the IMEI (International Mobile Equipment Identity), IP address, http headers, and even screen size and communication channels can be used. The IMEI is used by a Telco to block service provisioning of a lost phone.

4. MALWARE, ATTACKS ON MOBILE OS, APPS, NETWORK.

Malware is software used or programmed by attackers to disrupt computer operation, gather sensitive information,

(Continued from page 11)

or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of malicious, hostile or intrusive software (definition by wikipedia.org/wiki/Malware)

Malware includes computer viruses, worms, Trojan horses, rootkits, key-loggers, diallers, spyware, adware, rogue software, ransomware and other malicious programs. Most active malwares on smartphones are usually worms and Trojans rather than viruses. Once malware has infected a smartphone, it always aims to spread one way or another. Here follow some definitions in general use and also important for smartphones:

- Trojan (horse) is a program that allows external users to connect discreetly for malicious actions.
- Worm is a program that reproduces on multiple computers across a network. Infected Apps (e.g. from unofficial sites) can easily spread worms on multiple mobiles
- Viruses are designed to spread to other computers by inserting itself into legitimate programs and running programs in parallel.
- Rootkits software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable privileged access to a smartphone.
- Key-logger is software to record (or log) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware of these actions
- Diallers can be designed to connect to premium-rate numbers to make money from the calls
- Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge
- Rogue software (randsomware) misleads users into paying money for fake or simulated removal of malware.

Another category of messaging which is intruding and disturbing users is spam. This affects all users of fixed and mobile communication. Here the telecom operator or service provider can play a role. Recognition of messaging spam and the labelling can be carried out in the message service centre, the message gateway, the charging server and/or any network-related entities. Blacklists/whitelists could be deployed by the network operators to block recognized or reported spammers. Technologies such as filtering are appropriate for deployment by the network operators. Technologies that need an analysis of information collected by the network operator have to be deployed on the network side. These include traffic statistics, analysis of call data records, duplicate content recognition, indication information recognition and analysis of messaging sending dispersion.

Much work on the network side of mobile security is done by the international standardisation organisations like the ITU (International Telecommunications Union) and 3GPP/ETSI (third Generation Partnership Project / European Telecommunication Standardisation Institute) The objective of recommendations is to protect the personal privacy of users and to improve information security of smartphones. Smartphone threats are categorized into vulnerabilities and attacks. In order to satisfy security objectives, a hierarchical security framework and relevant security considerations are developed for smartphones.

Mobile networks are in general well protected. However mobile networks have some weak points. The radio interface between the terminal equipment and the serving network represents a significant point of attack. The threats associated with attacks on the radio interface can be split into the following categories:

- unauthorised access to data;
- threats to integrity;
- denial of service;
- unauthorised access to services

Unauthorised access to data on the radio interface

- Eavesdropping user traffic
- Eavesdropping signalling or control data to access security management data for active system attacks
- Masquerading as telecom participant to intercept user traffic, signalling data or control data
- Passive traffic analysis to observe sessions time, rate, length, sources or destinations
- Active traffic analysis to initiate sessions and then obtain access to information

Threats to integrity

- Manipulation of user traffic
- Manipulation of signalling or control data:

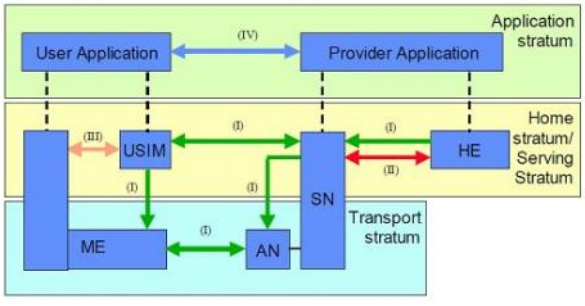
Denial of service attacks

- Physical intervention
- Protocol intervention

Unauthorised access to services

- Masquerading as another user or entity towards the network e.g. as a base station

3GPP/ETSI has paid much attention to the security aspects of mobile networks. Special security working groups have produced many Technical Specifications and Recommendations. They use a model architecture given below where layers are distinguished for Application, Home and



Overview of the 3GPP security architecture

Transport.

Attacks based on the mobile networks are focussed on breaking the encryption. 3GPP/ETSI has standardised block ciphers A5/3 and A5/4 also known as KASUMI or UEA1 which are much better than the current stream ci-

phers A5/1 and A5/2. After the attacker has broken the encryption algorithm of the mobile network, all unencrypted communication via the smartphone can be intercepted by the attacker. In general mobile networks itself are well protected against intruders. However, continuous improvements are required to cope with attackers.

Most smartphones have WiFi for access at home or at hotspots providing faster bitrates than mobile networks and at flat rate. Unauthorised WiFi access and eavesdropping (spying) the connection is easier than with mobile networks. Most WiFi connections or wireless LANs use WPA (WiFi Protected Access) based on the IEEE 802.11i standard. Users have to choose a 12 digit password which can be cracked, in particular when weak user passwords are used (which is often the case). Smartphones remember the accessed WiFi networks. This is a vulnerability as an attacker can twin a WiFi access with the same parameters, guiding the user to his network and steal his login parameters and eavesdrop unencrypted information.

Bluetooth access is another security concern. Unregistered services do not require authentication. An attacker only needs to connect to the port to take full control of the device. Registered use is safer.

5. THE POTENTIAL SMARTPHONE PROTECTION SOLUTIONS.

The first protection is always physical protection. Avoid by all possible means that the smartphone or tablet is stolen or misused. Don't leave it unattended on the table, in the car, in the pocket. Make it a natural habit to check its presence; it is your wallet, purse, private storage, business tool, and life saver.

Much malicious behaviour is allowed by the carelessness of the user. From simply not leaving the device without a password, to precise control of permissions granted to applications added to the smartphone, the user has a large responsibility in the cycle of security and should not be the vector of intrusion. This precaution is especially important if the user is an employee of a company that stores business data on the device. Instead of a password also biometric data can be used. Biometrics is a technique of identifying a person by means of recognition of the eye, face, or signature.

Some precautions are described hereafter to manage security on a smartphone.

Encrypted VPNs (Virtual Private Networks) provide secure end-to-end connections. IPSec, TLS (Transport Layer Security) and its predecessor, SSL (Secure Sockets Layer) used in https, are cryptographic protocols that provide communication security over the Internet. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Therefore https should be used for trusted transactions.

The next layer of security within a smartphone is at the level of the operating system. Beyond the usual roles of an operating system on a smartphone (e.g. resource management, scheduling processes), it must also establish the protocols for introducing external applications and data without extra risk.

If a malicious program manages to reach a device, it is necessary that the vulnerable area presented by the system be as small as possible. Sandboxing extends this idea to compartmentalize different processes, preventing them from interacting and damaging each other.

Android uses mechanisms of user process isolation based on Linux. This approach is based on a sandbox: while applications can be malicious, they cannot get out of the sandbox reserved for them by their identifiers, and thus cannot interfere with the proper functioning of the system. It is impossible for a process to end the process of another user; an application can thus not interfere with another application.

From the legacy of Linux, there are also file system permissions mechanisms. They help with sandboxing: a process cannot edit any files it wants. It is therefore not possible to freely corrupt files necessary for the operation of another application or system. Furthermore, in Android there is the method of locking memory permissions. It is not possible to change the permissions of files installed on the SD card from the phone, and consequently it is impossible to install applications.

Android is an open platform, designed to be securable. An owner breaking the root on his own device will not harm the security of Android which is based on the Linux kernel. Application developers have many security tools available including the used safe Java language. Apps are given their unique user identifier to protect its data. Users have to give explicit permission (accept) at App installation to use resources on the smartphone. However, these are often taken for granted by the user.

Finding and fixing security holes is done by a large group of experts who have great interest to provide secure applications in a secure environment.

The intrusion of a rootkit in the smartphone system is a great danger. It is important to be able to detect and prevent this. The intrusion could be a partial or complete bypass of the device security, and the acquisition of administrator rights by the attacker. Then nothing prevents the attacker to study or disable the safety features, deploy wanted applications, or spread a method of intrusion by a rootkit to more smartphones.

A defence mechanism in Apple is the Chain of trust in iOS. This relies on the signature of the different applications required to start the operating system, and a certificate signed by Apple. In the event that the signature checks are inconclusive, the device detects this and stops the boot-up.

Apple has chosen for a closed model where approved applications run on own hardware. Apple released an SDK (Software Development Kit) to fulfil the stringent requirements. Development is done in high-level Objective-C APIs to overcome some of the security threats in classic C (like buffer overflow). Apple Apps must be first approved before they get a valid code-signing certificate and can be distributed via the Apps store. This is a security boundary. Apple Apps uses sandboxing (or seatbelt) as well, preventing unsecure application interactions.

Memory protection prevents privilege escalation. If a process manages to reach the area allocated to other processes, it could write in the memory of a process with rights superior to his own, with root in the worst case, and perform actions which are beyond its permissions on the system.

Antivirus software can be deployed on a device to verify that it is not infected by a known threat, usually by signature detection software that detects malicious executable files. A firewall, meanwhile, can watch over the existing traffic on the network and ensure that a malicious application does not seek to communicate through it. It may equally verify that an installed application does not seek to

establish suspicious communication, which may prevent an intrusion attempt.

Resource monitoring in the smartphone can detect malicious applications. When an application passes the various security barriers, it can perform the actions for which it was designed. When such actions are triggered, the activity of a malicious application can be sometimes detected if one monitors the various resources used on the phone. This can be excess use of the battery, memory or communication channels.

Some malware is aimed at exhausting the energy resources of the phone. Monitoring the energy consumption of the phone can therefore be the way to detect certain malware applications.

Memory usage is inherent to any application. Though, if one finds that a substantial proportion of memory is used by an application, it may be flagged as suspicious.

On a smartphone, many applications are bound to connect via the network, as part of their normal operation. However, an application using much bandwidth can be strongly suspected of attempting to communicate a lot of information, and disseminate data to many other devices. This rises only a suspicion as legitimate applications like streaming video can be very resource-intensive in terms of network communications. Network traffic exchanged by phones can be monitored. One can place safeguards in network routing points in order to detect abnormal behaviour. As the mobile's use of network protocols is constrained, expected network data streams can be predicted (e.g. the protocol for sending SMS), which permits detection of anomalies in mobile networks. If an abnormality is found in the fluctuation of network data in the mobile networks, a potential threat can be quickly detected.

As is the case with e-mail exchanges, a spam campaign can be detected through means of mobile communications (SMS, MMS). It is therefore possible to detect and minimize this kind of attempt by filters deployed on network infrastructure that is relaying these messages. When installing applications, it is good to warn the user against sets of permissions that, grouped together, seem potentially dangerous, or at least suspicious.

Along with App stores appeared a new feature for mobile apps: remote revocation (withdrawal of an application). This procedure can remotely and globally uninstall an application, on any device that has it. This means the spread of a malicious application that managed to evade security checks can be immediately stopped when the threat is discovered.

New versions of various software components of a smartphone, including operating systems, are regularly published. They correct many flaws over time. Nevertheless, manufacturers often do not deploy these updates to their devices in a timely fashion, and sometimes not at all. Thus, vulnerabilities persist when they could be corrected, and if they are not, since they are known, they are easily exploitable.

A user should not believe everything that may be presented, as some information may be phishing or attempt to distribute a malicious application. It is therefore advisable to check the reputation of the application that you want to buy before actually installing it.

The mass distribution of applications is accompanied by the establishment of different permissions mechanisms for each operating system.

It is necessary to clarify these permissions mechanisms to users, as they differ from one system to another, and are not always easy to understand. In addition, it is rarely possible to modify a set of permissions requested by an application if the number of permissions is too great. But this last point is a source of risk because a user can grant rights to an application, far beyond the rights it needs. For example, a spreadsheet application does not require access to the geo-location service. The user must ensure the privileges required by an application during installation and should not accept the installation if requested rights are inconsistent.

Protection of a user's phone can be done through simple gestures and precautions, such as locking the smartphone when it is not in use, not leaving the device unattended, not trusting applications, not storing sensitive data, or encrypting sensitive data that cannot be separated from the device.

Smartphones have a large memory and can carry several gigabytes of data. The user must be careful about what data it carries and whether this should be protected. While it is usually not dramatic if a song is copied, a file containing bank information or business data can be more risky. The user must have the prudence to avoid the transmission of sensitive data on a smartphone, which can be easily stolen. Furthermore, when a user gets rid of a device, it must be assured that all personal data first is removed.

Apple provides only approved software on its own hardware. As said Apps are tested and monitored to fulfil the stringent Apple requirements

Google has an automated system that scans Android Apps for potential malware or unauthorized behaviour. Once an App is uploaded to Google by its developer but before it is published via the Android store, the code is scanned for known malware, including spyware and Trojan horses. Google looks for behaviours that match Apps which the company has previously decided are unacceptable. Some Apps are immediately denied entrance to the Android store; others are flagged for human review.

Things which should be done to dramatically reduce the risk of malware infections on an Android smartphone are:

- Use the official Android store play market instead of third-party App stores or websites. Turn off in settings the ability to install apps from unknown sources
- Check the publisher and App reviews before downloading.
- Pay attention to App permissions during the installation and check for an explanation of any suspicious permissions.
- Install an antivirus/security App.
- Be wary of phishing scams and malware via the Web browser or SMS messages.
- Be cautious if you root your device. Rooting allows to use some powerful Apps and even enhanced security functionality, but at the same time increases potential damage from infections.
- Prevent any malicious Apps from sending messages to a number that will automatically charge your account.

Summarising the precautions which should be done to increase the security on smartphones in general:

1. Lock the smartphone with a strong key or PIN. This may seem like an annoying feature to use, but it is highly valuable in protecting the data in the smartphone against theft. With accidentally losing the smartphone or theft, an unlocked smartphone gives

any thief complete access to every piece of data you access.

2. Download always only trustworthy Apps. One of the great things about smartphones is access to countless free and inexpensive Apps. Apps require some level of access to the data on the phone, which means some Apps could maliciously acquire access to secure areas and data they shouldn't need. So before downloading an App, read the reviews and research the App itself to determine if it is truly legit, and consider mobile security software.
3. Update when prompted. Updates can be quite annoying to endure. They are disruptive and tend to take a while to complete. Often the smartphone has to be connected to a computer or download the upgrade over a wireless connection, which is inconvenient. But avoiding these updates can leave the phone incredibly vulnerable. All developers try to close loopholes with these upgrades. In getting behind on an update, the smartphone is left open for attack.
4. Turn off GPS, Bluetooth and Wireless features, in particular personal hotspot which shares a mobile internet connection with other users. Disable them when they are not used. Not only are they constantly draining the battery (they will constantly be trying to locate wireless networks, other Bluetooth devices, and calculate location), they can also be routes for malicious content. A mobile data connection via a mobile network is better protected than other wireless connections like WiFi or Bluetooth. Also automatic connection with a (previous connected WiFi or Bluetooth) wireless link might better be disabled as this link might be spoofed.
5. Prepare for the worst using remote wipes, remote control and backups. This works only when an internet connection is available. So local protection remains important. What information would a thief have access to? What would be the damage on bank account and social networking accounts? If the phone were to be stolen, a remote wipe App would allow simply turn on the computer and access remote wipe settings via a web browser. Provided the internet connection has not been switched off, this software will remotely access the phone via a wireless or fixed line (WiFi) signal and return the smartphone to its factory settings, completely erasing all personal information.

6. WHO CARES, WHO PROVIDES SECURITY?

The first who is expected by the user to provide security for the smartphone and tablet is the ISP (Internet Service Provider) often in combination with the Telco who provides the connectivity. The user relies on ISP and Telco firewalls including SPAM filters and malware blocking. Sometimes this is an extra feature provided at additional cost. The number of published security incidents on smartphones is still rather low to raise concern with the users. However, this can change fast as smartphones are considered as attractive targets for intruders. Telcos can distinguish themselves by providing extra security as an additional service. However, not all security measures can be taken by the Telco. The user shall also pay more attention to security aspects.

BlackBerry provides a high level of security by its proprietary servers, generating encrypted and compressed push e-mail. The number of allowed log-in trials, remote wipe, allowed permissions and encryption for applications, files and memory make BlackBerry one of the best secured smartphones for business use.

Security on a workplace deals with technologies and secure ways of working for e-mail, internet use, instant messaging, social media, blogs, smartphones and tablets (including camera phones). It is also a way of handling these media by means of a corporate or business policy which should lead to greater security. Not everything should be allowed and some measures should be enforced like strong PINs, remote wipe and secured e-mail. It is this combination of actions and rules to provide optimal protection of vital private and business data.

Web Application Security by Web Application Firewalls (WAF) is promoted by the Open Web Application Security Project (OWASP). According to OWASP the following aspects should be considered as important for an organization:

- Access to personal data
- Access to confidential information
- Completion of critical business processes
- Attainment of critical (security) certifications

The CIS (Center for Internet Security) focusses on enhancing the cyber security readiness. Their website provides valuable information on security.

ISF (Information Security Forum) deals with information security on all kinds of platforms.

The ITU (International Telecommunications Union) Study Group 13 deals with "Future networks including mobile and NGN (Next Generation Networks)". The group is responsible for studies relating to the requirements, architecture, evolution and convergence of future networks. This includes International Mobile Telecommunications (IMT), wireless internet, convergence of mobile and fixed networks, mobility management, mobile multimedia network functions, internetworking, interoperability and enhancements to existing ITU T Recommendations on IMT.

IEEE (Institute of Electrical and Electronics Engineers) prepares standards for wireless communication including the well-known 802.11 family for wireless local area networks (WiFi) in the 2.4, 3.6, 5 and 60 GHz bands. IEEE-security issues a magazine and organises congresses and symposia on computer security.

TM Forum model for security mgmt of Telecom Operators

TeleManagement Forum provides a Cyber Security Model for Telecom Operators as a guidance concerning architecture, processes, information and data models, applications, interfaces and testing. As shown in the following figure it concerns the whole process chain from prevention to recovery, dealing with monitoring, analysis, detection, warning and remediating (see further details in the description of their model TR 172, given in the references section).

(Continued from page 15)

STOP. THINK. CONNECT.™ is the global cybersecurity awareness campaign launched in the US in 2010 to help all digital citizens stay safer and more secure online. Their guidelines for mobile devices are in line with the previous smartphone protection solutions.

In The Netherlands the National Cyber Security Center provides guidelines and recommendations for cyber security, including mobile communication. They contain valuable instructions to increase security with mobiles.

All these initiatives are directed towards more secure communication, including the smartphone.

7. CONCLUSIONS

Smartphones and tablets are replacing PCs and laptops for numerous tasks. With over 6.5 billion mobiles, including 2 billion smartphones and tablets, mobile operating systems and applications dominate the communication market. Transactions, including ordering goods, making reservations and payments, require much confidential information and need therefore a high level of security. Most users take security for granted. They expect that the telecom operator, mobile terminal and operating system provider like Apple-iOS, Google-Android or Microsoft-Windows provide enough measures and protection. They rely on courtesy of banks, Telcos, service providers or other companies in case attackers or intruders are capable to create financial damage, disturb their communication or business. Often attacks create havoc which is time consuming, frustrating and costly to repair.

Security protection comes first by our behaviour and caution. Preventing physical loss and unauthorised access is always the best protection. Then withstand temptation visiting unsecure sites or opening suspicious e-mails. Intruders often rely on psychological weaknesses, like curiosity, suspicion, greed and status. If the sender is not known or questionable, simply deleting the message is the best remedy.

The next barriers are some technical solutions. Firewalls, trusted connections (IPSec or TLS VPN), Anti-X protection programs, and malicious software effect monitoring will provide additional security. Anti-X is protection against virus, spyware, phishing, spam etc. Limiting access to memory, networks, vital data and other applications can restrict havoc. At this moment the security problems with mobile communications are still limited but growing fast. Smartphones and tablets have in general fewer resources than PCs and laptops to cope with the attackers and intruders. Though their processing capabilities and memories increase fast, it is questionable if this is enough to cope with the increased sophistication of malware and intrusions. Several smartphone protection solutions are proposed. However, new ways of attack emerge every day. Technical barriers can only partly provide protection.

Unfortunately people often take actions if it is too late. Therefore, recovery procedures, remote control and wipe, back-up, caution and spread of risks are all required in this new smartphone era. It is the responsibility of the user to select and implement proper security measures. Be it the selection of the type of smartphone, the OS, Telco, ISP, protection software or visited sites, it is the user's choice.

About the Author.

Huib Ekkelenkamp graduated at Delft University of Technology in 1978 in the field of telecommunications. He joined KPN with research on digital optical fibre transmission systems. He worked in several countries for the international consulting organisation of KPN. He spent many years in the Far East and worked in Indonesia in the area of telecom network planning. After his return to Europe he headed a KPN consulting team for telecom business customers. He managed telecom consulting projects in Central and Eastern Europe and was involved in international acquisitions of KPN. In 2001 he became in KPN responsible for ICT business development. Currently he is in Atos Origin as Telecom Solution Manager with a team responsible for business and solutions development. His main professional areas of interest are Mobile communication, Fixed-Mobile Convergence, Next Generation Intelligent Networks, IP Multimedia Subsystems (IMS), Cloud Computing, Operational Support Systems and Service Delivery Environments.

FITCE Forum

http://www.fitce.org

Editor: Barry Reynolds E-Mail: news@fitce.org

Editorial Board: FITCE Marketing Group.

FITCE values and Aims

1. Keeping in touch with leading edge ICT developments.
2. Ensuring that our Members benefit from the experience acquired by other Members in all ICT fields.
3. Building strong cultural and business ties between European ICT Professionals.
4. Ensuring that Young Professionals are able to use FITCE as a valued resource in their career development.