



SecurIST Report



Joint Workshop Security & Dependability in Mobile and Wireless: *Future requirements for R&D*



Brussels
11/12 May 2006

Project details

Project no. 004547

Project acronym: SecurIST

Project title: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D (*Steering Committee for a European Security & Dependability Taskforce*)

Instrument: Coordinating Action

Priority: SIXTH FRAMEWORK PROGRAMME

PRIORITY 2

Information Society Technologies

Deliverable reference number and title

Joint SecurIST, Mobile and Wireless Workshop report

Event date: 11/12th May, 2006

Organisation name of lead contractor for this deliverable:

Waterford Institute of Technology

Revision: Issue 1.0

Table of contents

Project details	2
1 Plenary 1.....	5
1.1 Welcome, Workshop Objectives and Format.....	5
1.2 Agenda and plans for the workshop	6
1.3 Presentations.....	9
2 Overview of working Streams.....	16
2.1 Introduction	16
2.2 Stream structures (carried out for each of three streams).....	18
2.3 Method used for Gathering Information.....	19
3 Working Stream 1: Secure Technologies & Mechanisms & Virtualisation.....	20
3.1 Participants	20
3.2 Executive Summary	20
3.3 Stream 1 Scenarios	21
3.4 Summary of Topic areas.....	27
3.5 Final results	27
4 Working Stream 2: Mobile Software & Services & Information.....	29
4.1 Executive Summary of the Chair	29
4.2 Participants	29
4.3 Stream 2 Overview	29
4.4 Stream 2 Scenarios	30
4.5 Stream 2 Workshop results - Extended Summary.....	31
5 Working Stream 3 – Mobile perspective End User needs.....	34
5.1 Executive Summary	34
5.2 Stream 3 Overview	34
5.3 Session Summaries.....	37

Workshop Participants

Carl-Johan Aakerblom,
Eyal Adar, ITCON
Francois Armand, Saluna
Atta Badii, SecurIST STF, FASTMATCH,
University of Reading, UK
Giuseppe Bianchi, Uni Roma
Rolf Blom,, Ericsson
Karima Boudaoud, University of Nice
Mauro Caporuscio, Plastic
Jim Clarke, Waterford Institute of Technology
Tanguy De Lestre,
Willie Donnelly, SecurIST, WIT/TSSG
Boris Dragovich, CREATE-NET
Stephan Engberg, Priway
Bosco Fernandes, Siemens
Nuno Ferreira Neves, Universidade de Lisboa
Chandana Gamage, VUA
Antonio Gómez Skarmeta, Universidad de
Murcia Spain
Bernard Hämmerli, Acris GmbH
Ian Herwono, BT
Mario Hoffmann, Fraunhofer SIT
Keith Howker, Vodafone
Robert Istepanian,
David-Olivier Jacquot-Chiffelle, Virtual
Identity and Privacy Research Center
Sabbah Jassim, U. Buckingham Business
School
Nigel Jefferies, Vodafone
Susana Jurado, Telefónica I+D
Yiannis Kliafas, Athens Technology Centre
Thomas Kohler, UBS AG
Tamas Kolossa,
Iordanis Koutsopoulos, CERTH-UTH
Michael Kreuteer, TU Darmstadt
Antonio Kung, Trialog
Latif Ladid, SecurIST
Ralf Lindner, Fraunhofer ISI
Javier Lopez, University of Malaga
Gordana Mijic,
Kamoun Mohamed, Motorola
Jean-Fr Molderez, CETIC
Simin Nadjm-Tehrani, Linköping University
Syed Naqvi, CETIC
Mark Nijdam, BT
Pierre Parrend, INRIA
L.F. Pau, RSM, Rotterdam, School of
Management and PRIME
Brian Randell, University of Newcastle
Sathya Rao, Telscom
Robert Ricci, Informa
Michel Riguidel, ENST
Thomas Roessler, W3C
Tobias Scherner, Uni Frankfurt, M-Lehrstuhl
Peter Schoo, DoCoMo, Eurolabs
Thomas Skordas, IST D4 EC
Alan Stanley, Information Security Forum
Peter Stuckmann, D1, European Commission
Bart Van Caenegem, IST D4 EC
Hu Wang, Huawei

The full set of working results from the three streams is included in the [Annex](#)

1 Plenary 1

1.1 Welcome, Workshop Objectives and Format

Dr. William Donnelly, Waterford Institute of Technology.

The idea for this Workshop was borne at the IST Mobile & Wireless Joint B3G-SA & Security Clusters workshop held in September 2005. This workshop gave an opportunity for presentations of security work and challenges of existing mobile and wireless projects, but it did not set out to look at the needs of future European R&D, which is the principal focus of the FP6 SecurIST project. The September 2005 Workshop was attended by Bosco Fernandes of Siemens and Willie Donnelly of Waterford Institute of Technology, both from the SecurIST project. As a result, the SecurIST project engaged the relevant people about a potential follow-up event and after receiving very positive feedback, proposed to organise such a workshop. Those ultimately consulted and involved were:-

- European Commission Units D1 (Communications Technologies) and D4 (ICT for Trust and Security);
- new and existing FP6 projects and the Security and B3G-SA Clusters;
- the eMobility Technology Platform;
- the WWRF Security SIG;
- invited mobile and wireless and security and dependability experts;
- the SecurIST project itself, both as organiser and contributors – indeed, many members of the Security and Dependability Task Force and SecurIST Advisory Board already fall into the above mentioned groups.

Dr. Donnelly presented some of the challenges to be addressed during the Workshop. For example, the emergence of open service-centric platforms, such as service oriented architectures (SOA) using web services, provides major opportunities to position the European software industry at the heart of the emerging information society. However, the uptake of solutions based on software and services by industry, especially in the mobile and wireless environments, are dependent on all stakeholders (industry and end users) confidence in their security and dependability. Therefore, the main goal of this Workshop was to gather the experts to elaborate and discuss the challenges and priorities that must be addressed by the Mobile and Wireless and Security and Dependability communities in both the medium and long term of the 7th Framework programme. The outputs of the workshop can directly contribute to the development of the strategy and roadmap for future European R&D in the field of security and dependability. The workshop schedule was designed over two days to allow for real in depth working discussions and debate about where European R&D in the field of ICT security and dependability in Mobile and Wireless environments should be heading – what really matters, what are the priorities, and what needs to be done specifically as *European R&D* in this area.

The talk concluded with a video providing a scenario from the IP Daidalos project. This project is about Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services. The scenario portrayed a mobile worker accessing services throughout the day, which requires the integration of complementary network technologies to provide pervasive and user-centred access to these services.

1.2 Agenda and plans for the workshop

May 11th, 2006 Joint SecurIST, Mobile & Wireless Workshop, Brussels

13:30 – 14:00	Registration
14:00 – 14:15	Welcome Workshop objectives and format Willie Donnelly
14:15 – 14:30	Joint SecurIST & Mobile and Wireless Workshop: ‘Setting the scene’ Thomas Skordas, European Commission
14:30-15:30	Chair: Dr. Willie Donnelly Keynote Speakers: Nigel Jefferies, Vodafone Stephan Engberg, SecurIST Advisory Board
15:30 – 15:45	Coffee break
15:45– 17:45	Workshop streams (parallel)

<p>Stream 1 Secure Technologies & Mechanisms & Virtualisation Co-Chairs: Nigel Jefferies, Vodafone Bosco Fernandes, Siemens Rapporteur: Sathya Rao, Telscom</p>	<p>Topics</p> <ul style="list-style-type: none"> • Architecture • Protocols • Secure software and execution environment including O/S • Network Dynamics • Wireless access • Business models • Secure and dependable end-to-end network protocols and applications • Cryptographic mechanisms • Device and network protection • Convergence • RFID • Authenticity • Trusted neighbourhood • MIPv6 • Legacy
---	--

<p>Stream 2</p> <p>Mobile Software & Services & Information</p> <p>Co-Chairs: Latif Ladid, SecurIST Nuno Ferreira Neves, FCUL</p> <p>Rapporteur : Jim Clarke, WIT</p>	<p>Topics</p> <ul style="list-style-type: none"> • Trusted creation • Certification • Security of web services • Software applications – s/w design methodologies • Middleware • Key Management • Secure transaction management • Unified Digital Rights Management • Code • Safe and secure software download • Usability • Awareness creation • Heterogeneity • Trusted execution • Terminal dynamics & data
--	--

<p>Stream 3</p> <p>Mobile perspective</p> <p>End User needs</p> <p>Co-Chairs: Bernhard Haemmerli, Acris GmbH Alan Stanley, Information Security Forum</p> <p>Rapporteur: Keith Howker</p>	<p>Topics</p> <ul style="list-style-type: none"> • Identity management • Privacy • Anti-fraud & local interception • Usability • Corporate identity • Compliance engineering • Transparent and flexible Service Level Agreements • Secure Billing • Data protection (confidentiality & Integrity) • Secure user profile and context information exchange • Access of information (Access control models) • Citizen empowerment
<p>17:45-18:00</p>	<p>Closure for first day – Willie Donnelly</p>

May 12th, 2005 08:30 Start

08:30-08:40	Welcome – Willie Donnelly Objectives of Workshop and format for second day
08:40-09:45	Keynote speakers Thomas Kohler- UBS AG Information Risk Control 'A Vision of Banking in 2015' Piotr Cofta, Mobility research centre, BT Ralph Lindner – SWAMI, Fraunhofer Institute for Systems & Innovation Research
09:45-10:45	Parallel Streams – continued – Session 2 Continuation of working streams from 11 th May
10:45 – 11:00	Coffee break
11:00-13:00	Parallel Streams – continued – Session 3 Continuation of working sessions, chairs and rapporteurs as per morning sessions The last session will focus on conclusions and recommendations as input to the vision, roundtable session.
13:00 -14:00	Lunch
14:00-16:00	Presentation of findings from working groups & Vision Roundtable session Rapporteurs present findings from workshop and distribute initial document for discussion Open questions for workshop participants
16:00-16:15	Conclusions (Willie Donnelly)

1.3 Presentations

Each day during the workshop a number of keynote speakers presented on a range of topics, eMobility, Visionary Banking, Trust, Ambient Intelligence. A summary of the presentations are given in this report and the presentations are available on www.securitytaskforce.org.

1.3.1 eMobility - Views of security from a technology platform

Nigel Jefferies, Vodafone

(please also see [presentation material](#) on workshop website)

The eMobility Technology Platform (www.emobility.org) is an industry-led platform whose objective is the drawing up of a Strategic Research Agenda (SRA) for Europe and to achieve critical mass for research and innovation. The platform was initiated in 2003 by Commissioner Liikanen as one of a number of working groups set up to represent the consolidated view of the industrial and academic researcher community. It held its public launch in March 2005 and has since conducted a number of events to present and develop its SRA.

The vision of the eMobility platform is to

- support the Lisbon Strategy for a competitive, knowledge-based economy
- drive future technology development in mobile/wireless communications to serve Europe's citizens and economy
- confirm the key role of scientific research & technological development for economic growth
- enhance cooperation between industry players, the research community and public authorities
- provide input for future European R&D programmes.

eMobility addresses three principle elements of future mobile and wireless communication systems – Simplicity, Efficiency and Trust (SET) - and the presentation concentrated principally on the Trust element.

From the perspective of the eMobility platform, the objective of Trust is to “provide any network, any device, with relevant content and context in a secure and trustworthy manner”. This includes a number of other important elements including seamless user experience, dependability, ubiquitous connectivity and ubiquitous services. The definition of and requirements for Trust and related concepts can be found in the presentation material <http://www.securitytaskforce.org/dmdocs/Nigel.pdf>

The eMobility Strategic Research Agenda is a living document with regular updates and the first release was in June 2004, and the latest in November 2005. The research challenges identified in the SRA were presented in detail. In summary, trust and associated concepts are critical to the success of future mobile networks and services, establishing clear definitions of the problems is difficult and it is recognised that more contributions are needed to establish a real ‘agenda’. It was for this reason that the eMobility platform were supportive of today's workshop.

Upcoming events were presented:

–May 2006 – SRA workshop, Brussels

–June 2006 – next version of SRA

–November 2006 – General Assembly in Heidelberg

If you would like to contribute, please use the eMobility WIKI at

http://wiki.ist-emobility.org/index.php/Main_Page Please contribute by the end of May 2006 to ensure inclusion in the new version of the SRA.

1.3.2 Changing Security Paradigms; from Trusted to Trustworthy computing http://www.securitytaskforce.org/dmdocs/Security_Wireless_workshop_Engberg_20060511.pdf

Stephan Engberg, Security Advisory Board & PriWay

Please see [presentation material](#) on the project website.

1.3.3 Summary of Presentation "Banking in 2015 and its Impact on Technology, namely on Mobile Technology"

Thomas Kohler, UBS AG

The aim of the presentation is to describe a compelling future banking environment based on 6 trends which are visible and which are influencing not only the Banking Industry but the service industry, as a whole. The trends are:

- Level of self-service will be significantly higher than today.
- Ubiquitous and mobile banking will be strong market drivers.
- Industrialisation of the value creation chain in banking.
- Increased readiness of Service Providers or Banks.
- Investments in technology will further growth.
- Security and Privacy in both the clients and the client advisors behaviour will be a key success factor for banking.

Mobile penetration in the EU countries is very high which is a sound basis for supporting some of the trends such as e.g. ubiquitous banking allowing the clients to do banking where ever and when ever they wish.

The industrialisation of the value creation chain will allow new service provider to step-in and to support parts of a business process. In order to allow this to happen, the necessary data is not stored with one or just a few Banks, but with the users themselves. Only this would allow a highly split-up business process to successfully run. The big issue however is that today's mobiles are not broadly equipped with the necessary features to support this concept of mobile data vaults. Further security mechanisms to support questions such as

- something I have (certificate)
- something I know (PIN)
- something I am (e.g. fingerprint, iris scan, speaker / voice recognition)
- something I do (I'm still the authenticated user by dynamic signature, pace analysis, ...)
- somewhere I am (context sensitive based on geographical location / environment) will have to be developed and rolled-out to the clients.

As a consequence of the industrialisation, firms will have to strictly focus on a few core competencies – the rest will be in-sourced from third party providers. What could be the role of the mobile service providers? Isn't e.g. placing an order at a stock exchange a kind of commodity which could be easily fulfilled by non-bank providers?

Time-to-market pressure will require a component based application architecture. Re-usability will see a revival. This is in my view another area where mobile communication providers could take a share: repetitive services which require an almost 100% availability, almost 100% reliability, non-repudiation, and not to forget: almost 100 % security.

The Service Provider or the Bank is a virtual partner or a virtual portal consolidating all personalised services required to satisfy the client. This requires the Service Providers or Banks to co-operate and to exchange data of their clients instantly, triggered-off by the client. This requires a type of applications which is network bound and which is capable to securely exchanging data on behalf of the requesting client. What device do we need for network bound applications if not a mobile or any

sort of a portable device? But again: this is much more than telephony and some office applications. This is about real banking applications running on a mobile device where this device is in one instance a host, in another instance a terminal and in another one a communication bridge. In my view, a mobile device will become an integral part of a highly dispersed business transaction!

The split-up of the value chain will foster a higher level of co-operation between Banks and Service Providers requiring application based interaction between the involved parties over a network which is formed in a real-time mode. This will be possible based on a regulatory framework which will more and more be harmonised.

Not every place is a secure place: there is indeed a difference if I do business in my protected home compared to a plane, waiting room, restaurant, etc. AND: we should not forget the travelling banking clients. He is not supposed to do every Business Transaction from every place. It could well be that the provider normally used does not have the right to accept an order in a different country. A solution to that issue could be a secure delegation of my rights to a secure process in my home jurisdiction. This is not possible to my knowledge and this would definitely again involve a high security, authenticity, integrity, availability and communication aspects. Today: we simply lack the mechanisms and processes. But tomorrow?

Geographical issues are fostering legal and regulatory issues. Even in the EU, the banking regulations are quite different from country to country and have to be fully adhered to. In the future I see a more harmonised legal and regulatory environment, at least in Europe. Instead of nation wide regulations, I see continent wide harmonisation, which is a huge step towards the right direction.

Honestly, I'm convinced that the trends outlined will become reality, sooner or later. However, I'm not that convinced of the direct impact on the mobile industry. However, the trend to a mobile society is visible already now but currently neither the necessary security measures nor the infrastructure nor the architecture nor the technology are place to support this transition.

1.3.4 Trust in a virtual world

Piotr Cofta, BT (piotr.cofta@bt.com)

Mobility is not about 4G and convergence is not about all-IP network. They are both about **virtualisations - the re-defining process** where resources are re-partitioned according to new needs. Mobility creates virtual space by removing traditional constraints while imposing its own (coverage, speed etc). Convergence re-purposes combines communication technologies to deliver newly packed uniform services.

Virtualisation has several potent drivers: technical freedom, innovation enablement, optimisation of investment, protection of core assets or lowering cost of ownership. It will stay with us, even though from security perspective, however, virtualisation adds new layers of complexity and make more convenient to forget about old errors.

Looking at mobility and convergence from security perspective we can see that mobility bypasses the physical security perimeter while convergence bypasses the logical one. Information within the **device is suddenly exposed to heightened level of treats** coming from driving-by attackers, dual-mode handsets or unmanaged networks. The walled garden of server rooms and GSM networks has been limiting - but it has been secure.

There are **three types of reactions** that we can see from the research community: 'An army of one' tries to protect the 'last ditch' - the device in a process of de-perimeterisation. 'Invisible hand of market' tries to implement social techniques to manage risk. Finally 'Battleship Galactica' acknowledges the situation by improving the recognition and response to attacks.

The real challenge is however to see the situation in a new lights and to **re-define security and trust for the virtualised world**. This require the understating of the relationship between those two concepts. Security is built on trust in particular elements that cannot be controlled. trust is built on security as it restricts the area that one should worry about. They are in a circular and spiral-like relationship leading to increased confidence in both technology and society.

Looking at virtualisation, we can see that security and trust are treated differently. Security is a core building block of virtualisation, which makes research in virtual security promising and desired. Virtualisation however erodes trust so that research in virtual trust are increasingly important (even though probably less glamorous). **Virtual trust should be the main research focus.**

Future research in virtual trust may follow the three different directions: 'An army of one' may turn to look for the reliable source of trust. 'Invisible hand of market' will formalise social perception of trust while 'Battleship Galactica' will improve the management of trust relationships.

Mobility can offer some valuable insight in virtual trust: SIM can become a pervasive source of trust; customer management can evolve into trust in mixed societies (human and otherwise) while network operation can be leveraged to support the convergent trust management.

1.3.5 SWAMI – Safeguards in a World of Ambient Intelligence

Ralph Lindner, Fraunhofer Institute for Systems and Innovation Research (ISI)

Privacy, identity, security, trust, and digital divide will become key issues in the emerging world of Ambient Intelligence (AmI). A growing part of the research and development community clearly recognises the inherent challenges that invisible, intuitive and pervasive systems of networked computers and sensors hold for social norms and values.

SWAMI – Safeguards in a World of Ambient Intelligence is an EU-funded research project with the purpose of identifying the social, legal, economic and ethical implications related to AmI. Based on extensive analysis of potential threats and vulnerabilities the technology might impose, the main objective is to develop research and policy options on how to build into future Information Society services and systems the safeguards needed to ensure user control and broad acceptance (project website: <http://swami.jrc.es>).

Background and vision of AmI

AmI describes a vision of the future Information Society as the convergence of ubiquitous computing, ubiquitous communication and interfaces adapting to the needs of the user. People are surrounded by intelligent, intuitive interfaces that are embedded in every-day objects and an environment that is capable of recognising and responding to the users in a seamless, unobtrusive and often invisible manner.

The most publicised visions and scenarios paint the AmI future in bright colours; in these visions, the applications always perform as desired and to the benefit of all users. While the SWAMI consortium believes that AmI holds many chances in terms of efficiency, user-friendliness and comfort, this technology is also associated with serious problems and risks:

- Firstly, significant portions of our daily activities need to be recorded, collected and tracked if the envisioned personalised services are to be made available;
- This will, secondly, increase the sheer *quantity* of personalised data in circulation in hitherto unknown dimensions;
- Thirdly, not only the quantity, but also the *quality* of the data will change due to the introduction of perceptual and biometric interfaces. Moreover, the tremendous amounts of personalised information in circulation may increasingly be linked, re-processed and re-used for secondary purposes.

The SWAMI project

The project's main tasks are:

- State-of-the-art-overview: In order to better understand the directions of thinking about AmI and its inherent threats, more than 70 R&D projects and roadmaps, many of which containing scenarios, was undertaken;
- Development of four “dark” scenarios in order to highlight potential problems in different settings

- Identification of major threats and vulnerabilities and the formulation of feasible safeguards and policy options in different domains (technical, socio-economic, legal).

“Dark” scenarios

The SWAMI scenarios have been developed in ways quite similar to other scenario exercises. The main difference is that SWAMI focused on *dark* situations, i.e., situations that enable us to highlight threats and vulnerabilities related to AmI. In short, the scenarios have the objective to identify important things that can go wrong, thereby calling attention to an AmI vision we do NOT want to become reality.

From a methodological perspective, the SWAMI scenarios are so-called trend or reference scenarios – these are extrapolations from current trends. They do not depict extreme, impossible or unlikely futures; and they are not neo-luddite. On the contrary, the dark scenarios are intended to be constructive towards realising AmI.

The four SWAMI scenarios cover the four quadrants unfolded by the combination of the individual–societal axis and the private–public axis. The scenarios can be briefly summarised as follows:

- Dark scenario 1: A typical family in different environments – presents AmI vulnerabilities in the life of a typical family moving through different environments. It introduces dark situations in the smart home, at work and while taking a lunch break in a park.
- Dark scenario 2: Seniors on a journey – also references a family but focuses more specifically on senior citizens on a bus tour. An exploited vulnerability in the traffic management system causes an accident, raising many different problems related to both travel and health AmI systems.
- Dark scenario 3: Corporate boardroom & court case – takes a different stance, involving a data-aggregating company that becomes victim of theft of the personal data which fuel its core business. Given its dominant position in the market, the company wants to cover this up but will face the courtroom two years later.
- Dark scenario 4: Risk society – suggests AmI as risk society portrayed from the studios of a morning news programme. It presents an action group against personalised profiling; the digital divide at a global scale and related to environmental concerns; the possible vulnerabilities of AmI traffic systems and crowd management in an AmI environment.

The technologies and devices used in the scenarios include embedded tags, sensors/actuators, biometrics, implants, smart dust etc. Among the applications built into the situations are location based services, spy ware, DRM, communication management systems, health monitoring devices, profiling and personalisation, and targeted marketing. The issues raised include loss of control, human factors in security, exclusion, dependencies, complex risk assessment, concentrations of power, digital divide, disproportionate actions based on profiling etc.

Threats and vulnerabilities in AmI

The main objective of the analysis of existing studies on the future of AmI and the scenario exercise was to identify the major threats and vulnerabilities (T&Vs) associated with the technology and its applications. The key areas in which the T&Vs are most likely to emerge are related to the issues of privacy, identity, security, trust and digital divide. Of course, many of the identified T&Vs are strongly interrelated and should not be viewed in isolation. In the following, a selection of major T&Vs in the key areas is briefly presented:

- Privacy: hackers, attackers and malware, function creep, surveillance, lack of public awareness
- Identity: identity-related crime, exploitation of data-linkages by industry and governments
- Security: unforeseen behaviour of complex systems due to insufficient design, internal complexity, lack of user-friendliness
- Trust: malicious actions, inadequate profiling for personalised services, loss of control, service denial and discrimination, victimisation

- Digital divide: accumulation of socio-economic disparities and knowledge gaps, system dependencies, exclusion and discrimination

The multiplicity of T&Vs needs to be addressed by a multiplicity of safeguards. In many instances, more than one safeguard is needed to counteract a single threat; and in other instances, a single safeguard addresses numerous T&Vs at the same time. The safeguards proposed by SWAMI are grouped into three domains: the technological, the socio-economic and the legal. The safeguards, policy and research options and recommendations to the European Commission will be presented in detail in the next project deliverable which will be made available at the end of July 2006.

Ralf Lindner

Fraunhofer Institute for Systems and Innovation Research (ISI)
ralf.lindner@isi.fraunhofer.de
www.isi.fraunhofer.de

- The SWAMI project is carried out (Feb. 2005 – July 2006) within the Sixth Frame Work Programme of the European Commission. The interdisciplinary consortium consists of five partner institutions:
- Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany
- Free University Brussels, Centre for Law, Science, Technology & Social Studies, Belgium
- Joint Research Centre, Institute for Prospective Technological Studies, Seville, Spain
- Technical Research Centre of Finland VTT Electronics, Oulu, Finland
- Trilateral Research and Consulting, London, UK
- Project deliverables and the documentation of the SWAMI Final Conference are available at the project website: <http://swami.jrc.es>

1.3.6 Sevecom- Secure Vehicle Communication

Antonio Kung from Trialog requested to present another scenario that could be used for the Working group sessions of the Workshop. Mr. Kung presented the Sevecom project (Secure Vehicle Communication). This project is an eSafety project focusing on secure vehicle coordination (partners : Trialog, EPFL, U. Budapest BUTE, U.Ulm, Philips, DaimlerChrysler, Centro Riserche Fiat).

Objective of Sevecom

The objective of Sevecom is as follows: Vehicular communications (VC) and inter-vehicular communications (IVC) bring the promise of improved road safety and optimized road traffic through co-operative systems applications. A number of initiatives have been launched, such as the Car-2-Car consortium in Europe, or the DSRC in North America. A prerequisite for the successful deployment of vehicular communications is to make them secure. It is essential to make sure that life-critical information cannot be modified by an attacker; it should also protect as far as possible the privacy of the drivers and passengers. The specific operational environment (moving vehicles, sporadic connectivity, etc.) makes the problem very novel and challenging.

Sevecom will focus on communications specific to road traffic. This includes messages related to traffic information, anonymous safety-related messages, and liability-related messages. The following research and innovation work is foreseen:

- Identification of the variety of threats: attacker's model and potential vulnerabilities
- Specification of an architecture and of security mechanisms which provide the right level of protection. The following topics will be fully addressed : Key and identity management, Secure communication protocols (including secure routing), Tamper proof device and decision on crypto-system, Privacy. The following topics will be investigated in preparation of further work: Intrusion Detection, Data consistency, Secure positioning, Secure user interface.
- The definition of cryptographic primitives which take into account the specific operational environment.

Liaison through SecurIST

Sevecom believes that privacy and identity management have a fundamental architecture impact on the infrastructure. Sevecom is concerned that the Sevecom contribution should be "synchronised"/"compatible" with work on this area in other security projects. Antonio Kung made a request that liaison be enforced key projects dealing with privacy and identity management.

1.3.7 Summary of Presentation "Joint SecurIST & Mobile and Wireless Workshop: Setting the Scene"

Peter Stuckmann, Bart Van Caenegem & Thomas Skordas INFSO-D1 & INFSO-D4 European Commission

Disclaimer: The content of this contribution is the sole responsibility of the author and in no way represents the view of the European Commission or its services

After welcoming the participants, Thomas Skordas introduced the IST project portfolio, which is relevant to the workshop themes, supported by the two Units of the IST Programme involved in the organisation of this workshop, namely INFSO-D1 (Communication Technologies) and D4 (ICT for Trust and Security). Thomas described then the expectations that the two units had from this workshop and he concluded by informing the participants of the state of advancement of FP7 and of the first ICT-FP7 work programme for the period 2007-08.

Brief overview of IST-FP6 project portfolio of D1 and D4 related to the workshop themes:

- Unit D1 is supporting 96 RTD projects with around 420 M €EU funding. These belong to two main areas, Broadband technologies (41 projects, 157 M €EU funding) and Mobile & Wireless Systems beyond 3G (55 projects, 263 M €EU funding – of particular relevance to the workshop are the 10 projects belonging to the cluster “mobile service platforms”). Convergence in both these areas is seen from the service platform & network architecture perspective; the main technological trend is that broadband is becoming wireless while mobile is becoming broadband & pervasive.
- Unit D4 is funding 35 RTD projects with around 140 M €EU funding. Of particular relevance to the workshop are some projects under “resilient infrastructures” (research designed to enable the creation of resilient, self aware, self healing network and service infrastructures that would be tolerant of both accidental and malicious events), “immunity of networks” (research focusing on the design of secure and reliable wireless networks and trusted mobile services) and few more projects in the other clusters addressing user identification and authentication in mobile devices.

One can observe from the above that while in FP6 there are several projects in D1 and D4 but also in other IST Units (e.g., in FET, Embedded Systems and Software Technologies and in some application areas such as ICT for Health, Government, Transport or the Environment) that deal with security, dependability and trust (shortly, SDT) in mobile and wireless environments, overall the area is addressed in a rather fragmented way. Thomas noted that SDT is also transversal in a number of European Technology Platforms: e-Mobility (mobile & wireless communications, <http://www.emobility.eu.org/>), NESSI (software and services, <http://www.nessi-europe.com/>), but also ARTEMIS (embedded systems, <http://www.artemis-office.org/>), NEM (networked and electronic media, <http://www.nem-initiative.org/>) and ISI (Satellite communications, <http://www.isi-initiative.eu.org/>).

Given the above, Thomas stressed there is now a need to think about SDT in an integrated way and make informed decisions taking into consideration several perspectives that are driven by a future that will be ever more wireless, with more mobility and many more devices than we have today. What will then make the difference is: to be able to create and preserve *a secure, dependable and trustworthy communication and service infrastructure* which, based on a multitude of heterogeneous, interoperable communication networks, provides a host of (mobile) intelligent applications and services in different contexts that users want, any where, any time. Such infrastructure should be capable of supporting and servicing not only the few billions of users but also the trillions of connected sensors and other devices that will be everywhere around.

When designing SDT solutions for existing or future wireless and mobile network and service infrastructures, we need therefore to consider from the very beginning many different perspectives jointly: The end-user perspective; the networking technologies perspective; the service provisioning perspective; the SDT perspective; etc. Thomas then briefly explained these different perspectives which require a strong and durable collaboration between many different communities and linked these perspectives with the motivations & expectations that units D1 and D4 have from this workshop:

- (1) Serve as forum for concrete discussions aiming at identifying new joint areas for research, by bringing together inter-disciplinary constituencies from mobile & wireless networking technologies, software, services and SDT technologies as well as end users;
- (2) Providing input to the drafting of the strategic research agendas of the above mentioned technology platforms and in particular of e-Mobility and NESSI;
- (3) Providing input to the drafting of the FP7 work programme in the areas where units D1 and D4 are responsible; such input concerns both the R&D agenda but also ideas for large pilot projects that could deploy security and dependability and test how users react to them (experimental facilities for large scale demonstrators and test-beds, likely to be launched under FP7);
- (4) Finally, serve as a forum for building new Consortia around the identified critical priority areas, in view of the first FP7 Calls for proposals.

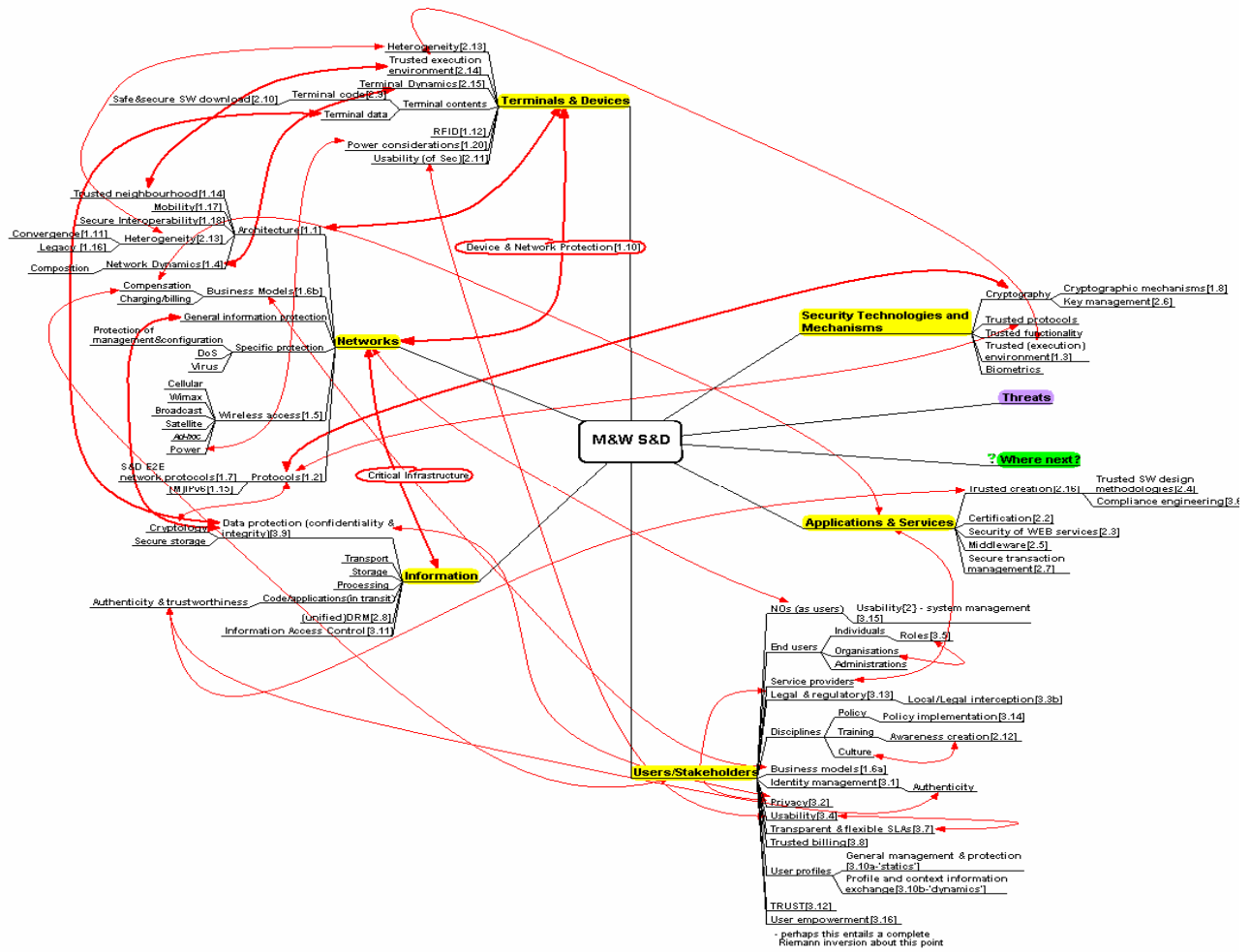
Thomas concluded his presentation by informing the participants of the state of advancement of FP7 and of the first ICT-FP7 work programme. A first draft of the work programme is expected to be ready before end July. The calendar is then as follows: discussions with the IST-Committee in September / October, formal adoption before Christmas and first calls for proposals just before or just after Christmas.

2 Overview of working Streams

2.1 Introduction

The Programme Committee spent a good deal of time discussing the format and themes to be covered within the working streams. It was recognized that the sessions would be comprised of heavy discussions and work being in a parallel fashion to try to capture as much valuable data as possible.

Input for the topics to be covered were also elicited from the participants who pre-registered to attend the workshop as they were asked to provide five hot topic areas of significant importance to them. These results were continuously factored into the makeup of the various working streams. The programming committee used this mind map to brainstorm the topics for the workshop and explore links.



D:\LocalCache\Projects\SecurIST\workshop\keyAreas\MM_02b.mmp - 31-05-2006

Figure 1: Mind Map of Workshop Working Streams

This diagram was used as the initial planning tool. It was updated to incorporate comments and ideas received during the registration process. The references [n.m] are to the document *Issues from Registration – Disposition to Topics* included in the [Annex](#) to this report.

2.2 Stream structures (carried out for each of three streams)

The Streams were each structured to follow a number of distinct phases including the inputs from all relevant parties as shown below.

Phase 1 Identify scope and landscape; initial selection of topics and priorities	Inputs <ul style="list-style-type: none"> initial consolidation by Programme Committee/Chairs/rapporteurs/ <i>ex five challenges</i> from registration process challenges from STF. Very important especially if champions for one or more of the topics not available. challenges, (planned) results, and problems from projects SecurIST Advisory board recommendations (for eventual mapping exercise (see below)) micro-presentations of key/favourite/obsessional issues
	Process <ul style="list-style-type: none"> take all inputs what is covered elsewhere (but should be noted) initial groupings etc. highlighting key people to topics.
	Output/results <ul style="list-style-type: none"> agreed themes and topics already in agreed template format.

templates were designed provide the specifications of these red interfaces – or rather the specification of the format of their content.

Phase 2 Explore selected landscape items; generate further insights; classify and categorise	Inputs <ul style="list-style-type: none"> outputs from Session 1 Euro-criteria/other filters e.g. Mobile and Wireless/S&D focus
	Process <ul style="list-style-type: none"> apply European priority and other filters judgement prioritise more detailed brainstorming/review/discussion of filtered topics etc.
	Output <ul style="list-style-type: none"> More details on themes and topics already in template format.

Phase 3 Analysis and reduction	Inputs <ul style="list-style-type: none"> outputs from Phase 2 template(s) for stream results
	Process <ul style="list-style-type: none"> Review Gather consensus Agree Mapping to/from SecurIST Advisory board recommendations report.
	Output <ul style="list-style-type: none"> Stream Report template published for presenting to Plenary session

Conclusions structure

Plenary: Conclusions & Recommendations	Inputs
	Process
	Outputs



Workshop Report

2.3 Method used for Gathering Information

It was decided to use the Brain Writing (BW) method to intensively gather the ideas (scenarios and challenges and priorities in this case) from all participants in parallel of inspired (in our case through keynotes) people down to paper.

In the first phase of BW, the whole group writes during 1-2 minutes his/her topics down in the theme columns. If a topic does not fit in a column, a new column with a heading is opened. After 1-2 minutes, the paper rotates and the expert is further inspired by the previous writer and the paper circulates around the entire group.

The second phase of BW is the Evaluation Phase. Each expert now has their original paper full of topic. The expert should now select 5—to 8 topics out of the paper in front of him and write this topics on a piece of paper, which can pinned later at the pin board. Each expert pin the topics at the pin board and explains the group why he has selected this topics. The group then discusses the selected topics and selects the 6 topics, which should be discussed further in detail.

3 Working Stream 1: Secure Technologies & Mechanisms & Virtualisation

Rapporteur: Sathya Rao, Telscom Consulting, Switzerland

3.1 Participants

The following people participated to the Working Group in Stream 1.

Nigel Jefferies, Vodafone (chair)
Bosco Fernandes, Siemens (Co-chair)
Sathya Rao, Telscom (Rapporteur)
Bart Van Caenegem, European Commission
Michel Riguidel, ENST
Peter Schoo, DoCoMo Eurolabs
Stephan Engberg, Priway
Iordanis Koutsopoulos, CERTH-UTH
Robert Ricci, Informa
Chandana Gamage, VUA
Kamoun Mohamed, Motorola
Michael Kreuteer, TU Darmstadt
HU Wang, Huawei
Mark Nijdam, BT
Rolf Blom, Ericsson
Francois Armand, Saluna

Note – the full results of Stream 1 Working Group may be found in Section 1 of the [Annex](#) to this report.

3.2 Executive Summary

Stream 1 addressed a group of topic areas mainly associated with security technologies, mechanisms, and architectures, and the challenges arising from them specific to mobility and wireless connection. The topics are listed in **Error! Reference source not found.**, below.

The big R&D challenges arise from the increasing size and capacity, and, hence, complexity, of a global information system. The expectation is going to be for best possible connection for the delivery of ambient intelligence – connection anytime, anywhere, to any person, service or device. The anticipated expansion of size and scope brings with them a de-perimeterisation, with boundaries between networks and domains blurring and disappearing. This in turn leads to de-centralisation of control and a consequent shift of responsibility towards the user and service provider that raises new security and dependability challenges.

Research fundamentals include the overall architectures at both the conceptual or *virtual* level, for high level design, modelling, and policy making, and at the *real* level concerning the working, functional entities and interfaces, and the communications between them. The requirements are for seamless roaming and interoperability in a dynamically shifting environment composed of a heterogeneous set of entities and services. At the network level, dynamic overlays – again dynamic – will deliver a wide spectrum of user needs.

Added to this requirements-perspective, there is still the need for commercial viability and the support for many possible business models and relationships. The essential concept of trust, fundamental to network connections, requires solid foundations for both the subjective, reputation-related, aspect and for the formal, possibly provable aspect of the *trusted* device or entity.

To support all this, there is the ongoing need for development of underlying engineering and research into new technologies to deliver higher security – but with increased performance, and at lower cost. These then need to be built into the protective mechanisms and countermeasures that can resist new forms of malicious attack as well as delivering the expected dependability in the increasingly complex

environment with its even faster increase of possibilities for malfunction and mis-operation. Protection of the system operation and services must also cover attack-resistance and fault-tolerance.

The Stream 1 working group generated and analysed many scenario challenges (section **Error! Reference source not found.**), and went on to prioritise their conclusions (section **Error! Reference source not found.**). The top priority items for the short, medium, and long terms were, respectively: for the trusted execution environment; for security to be independent of precise context (or, rather, to be optimised for the specific); and for complete architectural virtualisation.

3.3 Stream 1 Scenarios

The Working group was briefed by the two chairs on the methodologies to be used in developing scenarios and identifying the challenges and priorities based on their personal views, and then through iteration process on the ideas generated by the other. The activities started by holding a Brain Writing session on security technologies, mechanisms and virtualisation based scenarios that could be used for consolidating a set of scenarios that will become the basis for the next phase of the session on elaborating key challenges and priorities. Number of scenarios were identified by each participants. The list below provides so generated list of scenarios:

3.3.1 Participant: Francois Armand

Scenario 1: Independence from device:

Secure/Trustworthy access to whatever service a user needs should be available (although possibly in a slightly restricted form?) independently of the physical device it uses. So that he can depend on these services even after his "own" device has been lost, stolen or has simply run out of order; by borrowing the device of somebody who's trusting him.

Scenario 2: Many simultaneous usages:

A user may have multiple employers and may belong to different groups/communities. Hence being able to manage potentially conflicting security policies from the set of devices he has access to would be required by the employers/groups and also would permit the user to carry only one device at any time, although that device may not be the same during the day. (e.g. one for work, one for home...)

Scenario 3: Free Low Power Communications

In urban areas, with lot of wireless home renters: provide some bandwidth to pedestrians in the street to connect their device (phone or whatever) so that they don't need to establish any radio communication with a far away BTS and use less power from their battery.

3.3.2 Participant: Peter Schoo

1. Solutions that enable establishment of security associations between domains formed out of devices or NE and where for each domain one authority defines the NE of security polices. Managed & unmanaged networks. Able to be build on legacy.
2. Seamless and secure mobility management for heterogeneous radio access technologies. Radio technologies must not determine the Quality of Security as perceived by end user.
3. Solutions for cheap accounting (with all the other nice properties from non-repudiation to supporting anonymity by default), that cost actually so little that that flat rates are too expensive compared to them.

Wireless peer misbehaviour issues regardless of protocol (at all layers, physical, access, routing, application)

Detection

Countermeasures, isolation

Network resiliency

Trust-based – mechanisms + protocols for distributed peer communities

Reputation – based intrusion detection

Reputation – based QoS delivery

Formation of peer coalitions to enhance performance, games

Wireless DoS attacks (mild of brute-force jamming)

(Key challenge in wireless) Account for attack unpredictability + uncertainty, distinguish attack from occasional malfunctions.

Wireless peer-to-peer security

Intruder isolation, network protection

Incentives for complying with protocol

Punishment for the opposite

Challenge: peer is server + client at the same time

3.3.3 Participant: Chandana Gamage

Context sensitive information retrieved to personal mobile devices from central servers

E.g. If the user has just a mobile phone active, the system sends email sender identity and subject line. If the user has a notebook computer active, the system sends the messages as usual.

This could be extended to other applications and media like news, alerts, etc.

Important requirement is to have the context switching occur transparently automatically when user's environment change.

3.3.4 Participant: Rolf Blom

1. Secure platforms: OS, execution environments and services. Management of these platform Assurance measurements.
How to build and manage the trusted platform we need to implement secure servers.
2. Deployment of security system. Efficient methods to set up security in large and heterogeneous networks.
3. Attach resistance: Detection, prevention and design.

3.3.5 Participant: Mark Nijdam

1. Trusted core network, where trust coalitions with 3rd party service providers are established.
2. A security provider makes sure that a certain service can be trusted.
3. End users have control over a group of persons or identities, for each identity the end user is willing to take a certain level of risk.

3.3.6 Participant: Hu Wang

1. Heterogeneous networks they like to share cooperation (whatever kind). However, they may have different security policies. How should this be handled (in principle at first).
2. If end users are given the possibility to connect their electronic devices (of any kind) to the mobile network, probably using mobile terminals as gateway. Then the mobile terminal and the network should be resistant to any attacks generated from/by the electronic devices of users, which are one of control of the network operator, or terminal manufacturer.
3. There are security mechanisms built in the access networks. However, for some applications, user like to have end-to-end security. Is it meaningful to somehow reduce the unnecessary security processes, or just let it be? Practically it can be high cost to do this.

3.3.7 Participant: Bart van Caenegem

Scenario 1: Daidalos scenario:

Roaming services seamlessly between monopol unmanaged, centralized and ad hoc networks

Scenario 2:

interfacing with a trusted personal devices managing the roaming and the control with as little intervention of the user as possible between PDA – television – car navigator –etc.

Scenario 3:

future scenarios with RFID/sensor

Scenario 4:

- authentication to the network as per need to know
- anonymous
- pseudonymous
- business model?
- Who is billing-> the service provider not the infrastructure provider
- + end to end security to the service provider by end to end encryption
- Strong authentication to the trusted personal device and this device manages the communication with the service provider

3.3.8 Participant: Michael Kreutzer

Technology independent security

Defining “meta” security policies that can be (‘automatically’) mapped to technology-dependent implementations

New ways to cope with dynamics and lack of access to control infrastructures: self-x-properties:

- Self protection
- Self defence
- Self “healing”

3.3.9 Participant: Roberto Ricci

- Multimodal biometric identification techniques applied to network access, possibly through a Trusted Third Party
- Mutual biometric identity verification for P2P networks, possibly through TTP (e.g. for business-critical communications)
- Definition of a biometric identity “certificate” suitable to be used in network protocols and service access (“fuzzy” authorization, possibly refreshed dynamically)

3.3.10 Participant: Kamoun

Convergence between broadband fixed communication & wireless. As an example DSL subscriber with combined DSL/WIFI modem could share a fraction of his bandwidth in order to help operator to get a better wireless coverage.

Cooperative infrastructure with relays and routing terminals – a great increase for the available data rate but a big security/identification issue: which node should be trusted, how to handle security in a collaborative way.

3.3.11 Participant: Stephan Engberg

- Complete separation between identity and channel
- Zero trust loyalty programs
- Token paid infrastructure
- Dynamic threat level upgrade

- All-dynamic networks, all addressing is done indirectly using logical connections, purpose- kill denial or service attacks
- Each session a new IP (permanent)
- No reuse of IP-addresses
- No linkage between device IP addresses
- Zero trust in server “cynical” networking
- Access devices never identified
- 100% Edge networks (more likely the more central control)
- Virtual networks / open infrastructure full separation between physical channel and logical network
- Zero server side identification or non – server objects or persons
- Multi channel devices
- All communication devices should support min 2 different providers unlinkable simultaneously
-
- Meta - standardization
- Communication interfaces should describe their security model explicit – exchangeability + interoperability

3.3.12 Participant: Bosco Fernandes

Scenario 1:

Embedded system structures have constraints on system performance and cost. However, future architectures with more intelligence at the Edge could support these concepts:

Scenario 2:

Network Architecture Security

Harmonizing policies & procedures

Management

Scenario 3:

Improved IP security ← Mobile Networks

3.3.13 Participant: Nigel Jefferies

Scenario 1: Ubiquitous pervasiveness

Wireless devices are everywhere. Personal networks, sensors in every manufactured article, scattered “nodes” in the street. Users can collect information on they pass, interact remotely. Some as networks, some rely on ad hoc connections.

Scenario 2: The Death of the Perimeter

Networks, whether personal or corporate, will consist of shifting, mobile, heterogeneous collections of devices, lined by various different access core networks. Devices, nodes and users may leave or join at any time. There will be little or no central management.

Scenario 3: These Mean Streets

The Internet is a lawless place, users manage their own security as best as they can. The is little convergence with mobile when long consolidated operators still hold sway. VoIP never took off because of security, quality and commercial concerns.

3.3.14 Participant:: Sathya Rao

Scenario 1:

Virtualised security architecture, across independent security domains with clearly defined trusted info-spheres such as personal, enterprise and national

Scenario2 :

Security across Interoperable heterogeneous networks scenario independent of technologies and protocols used through appropriate middleware

Scenario 3:

Standards development and design of systems with security from the beginning to guarantee interoperability across multi-vendor systems.

Scenario 4:

Fault tolerant system design and deployment involving inbuilt intrusion detection and prevention functionality.

3.3.15 Participant: Michel Riguidel

Scenario 1: Security of a Mobile Community

Fleets of mobile sensors/actuators

Capturing data

Processing data

And then transporting information and knowledge

Security of several overlay networks

Heterogeneous technologies

Security policy

Scenario 1a – One Fleet

Scenario 1b – several cooperating Fleets

Scenario 2: Crisis Anticipation & Management (Security Management)

Enlarge and splitting in a bit of several domains, networks, etc.

Exchange & discussions ≠ CERT

log data

Computation, forecasting event (security...)

For Critical Infrastructure Protection, etc.

Scenario

Centralized | with protocol for Trusted Exchanges

Decentralized |

Multicast of Security Information -> (Europe Security Channel)

RFID – mobile objects Management (-> testbeds)

Scenario 3: Security of a Mobile Community (with Scarce Resources)

Security, mobility, scalability & maturity, traceability

After analysing all the scenarios provided by the participants, Mr. Rao produced 3 functional scenarios distributing all the features so identified, so that challenges and priority identification can be

simplified. These represent 1. user centric security 2. Trust centric security and 3. Zero trust:
empowering citizens paradigm.

3.4 Summary of Topic areas

The following functionalities were identified in proposing related challenges and priorities in this working group.

Architecture	Device and network protection
Protocols	Convergence
Secure software and execution environment including O/S	RFID
Cryptographic mechanisms	Authenticity
Network Dynamics	Trusted neighbourhood
Wireless access	MIPv6
Business models	Legacy

3.5 Final results

After identifying number of challenges (as shown in [Annex](#)), participants were asked to pick 3 major challenges from their view. Once this was collected on the chart, they were requested to vote on the priorities for short term, mid term and long term priorities.

The list below identified as the important challenges and prioritised issues for short, mid and long term.

1.Verifiable secure execution environment (Short term)

2.Meta security policies for independence of networks (midterm)

3.Virtualisation at architecture level (long term)

- 4.Seamless interoperability across heterogeneous networks (E2E)
- 5.Disruptive protocols to organise network surveillance
- 6.Quantitative trust infrastructure
- 7.Trusted Third Party Architecture
- 8.Protocols for energy efficiency and security
- 9.Reputation based protocols for QoS delivery and security
- 10.Issues in wireless P2P decentralised architecture
- 11.Distributed trust management in co-operative networks
- 12.Idnetity management across different networks including multiple identities
- 13.Embedded security protocols at all levels
- 14.Secure Innovative concepts for the future SIM
- 15.Secure user to device binding
- 16.Developing new IP with full security and mobility support
- 17.Security technologies for innovative business models
- 18.Use of data vaults and user oriented security architecture
- 19.Understand failures and misbehaviour of complex systems
- 20.Management of multiple environments with security policies on the device
- 21.Trusted computing, secure OS and TPMS
- 22.Attack resistance

23. Deployment for security

24. Self-X properties

25. Authentication security against Identity thefts

26. Resilient protocols to misbehaviour and misuse

4 Working Stream 2: Mobile Software & Services & Information

Rapporteur: Jim Clarke, Waterford Institute of Technology

4.1 Executive Summary of the Chair

By Latif Ladid, Chair of Stream 2. SecurIST project.

The mobile and wireless security based scenarios brainstormed and selected by the participants of this second stream were the mobile banking/payment/financial services, the mobile traveller accessing innovative services and innovative and empowering framework for user-based content provision. The ordinary users can become content creators and providers (i.e. creating content with cameras in their phones is just the beginning.).

16 challenges and priorities topic areas had been identified by the program committee and 10 more have been added by the working group in the stream 2.

The policy level recommendations, which rotate significantly around the view that security in mobile scenarios is a negotiated need between end users on one side and third party managed security and privacy service providers on the other side.

The need to specify security implementations inside any service specification and all security measures and agreements should be strictly sanctionable and enforceable legally. Significant research and real life testing with all involved stakeholders including policy makers is needed in real business environments.

There is an opportunity for the establishment of an EU-based content creation environment. The DRM required to establish a secure and effective content creation and provision environment does not necessary need new regulations; instead, it requires tools for identification and tracing of irregularities and content ownership.

Security should be a business enabler and not a showstopper and we should be capable of correlating security impact with business impact in real time with advanced security analysis tools.

4.2 Participants

The following people participated to the Working Group in Stream 2.

Adar, Eyal – ITCON
Boudaoud, Karima – University of Nice
Caporuscio, Mauro - Plastic
Clarke, Jim – Waterford Institute of Technology (Rapporteur)
Herwono, Ian – BT
Ladid, Latif - SecurIST – Chair Day 2
Molderez, Jean-Fr – CETIC
Naqvi, Syed – CETIC
Neves, Nuno Ferreira – FC/UL - Universidade de Lisboa, Faculdade de Ciencias (Chair Day 1)
Pau, L.F. – RSM Rotterdam school of management, and PRIME project
Randell, Brian– University of Newcastle
Schoo, Peter– DoCoMo Euro-Labs
Skordas, Thomas – European Commission

4.3 Stream 2 Overview

Based upon the Programme Committee brainstorming and factoring in the hot topics/themes for discussion from the registered participants, the themes that were included on the work sheets for Stream 2 were the following:

Trusted Creation	Secure Code
Certification	Safe and secure download

Security of Web services	Usability
Software applications – S/W design	Awareness creation
Middleware	Heterogeneity
Key management	Trusted Execution
Secure transaction management	Terminal dynamics and data.
Unified Digital Rights management	Others...

In addition to the elaboration of the above pre-determined themes, the participants were given the opportunity to add more themes that were also included for discussion and elaboration of key challenges and priorities during the sessions. For Stream 2, these included:

Business Impact	Grid Security
Spam	Network configuration context representation
Legal and ethical	Risk management
Dependability of the security architecture	Software Defined radio (SDR)
Outsourcing	Security/Trust of users

Note – the full results of Stream 2 Working Group may be found in Section 2 of the [Annex](#) to this report.

4.4 Stream 2 Scenarios

The Working group started by holding a Brain Writing session on mobile and wireless based scenarios that could be used for the next phase of the session on elaborating key challenges and priorities. Once the scenarios were elaborated and discussed, the participants voted on their preferred scenarios in order to prioritise the scenarios for discussion. The scenarios are summarized below and the number of votes received for each is also indicated.

The scenarios that were brainstormed by the participants of Stream 2 were:-

1. Mobile banking/payment/financial services as a replacement to traditional ATM or bank branch networks (e.g., third world countries). There is a significant EU opportunity in replacement of banks networks by with whomever is the wireless providers in this area for mass deployment with mass mobile security capabilities

Number of votes: 6

2. Mobile traveller accessing innovative services while abroad e.g. home based services (accessing smart home), e-government, eBanking, etc.)

Number of votes: 5

3. Complete framework for customer-centric based content provision. An already present scenario where the ordinary consumers have become content creators and providers (e.g. with the cameras in their phones). We are currently not empowering the user in the current content environment in the EU. We need to make the EU an environment of self created content provision with service help from a 3rd party or set of 3rd parties, which will have the task to manage security, privacy, IPR of content because content owners are not owners of the infrastructure.

Number of votes: 4

4. ISTAG scenarios on Ambient Intelligence. For example,
 - a. environmental scenario on CIIP
 - b. Emergency crisis management

Number of votes: 4

5. Automotive scenarios e.g. Daidalos scenario or V-2-V scenario as presented by Sevecom.

Number of votes: 3

6. Mobile environment access to the Grid computing environment. In order to move into the eCommerce sphere, the following must be addressed:

- a. Grid security
- b. We need to add significantly more data (content) into the GRID infrastructure (more than just biomedical and astrophysics data).

Number of votes: 3

8. Company to Company VPNs. Currently, very expensive and needs to be enhanced for other levels including:-
 - a. IP level
 - b. SLA levels
 - c. Trust models and metrics between companies.
 - d. One model of connectivity and security used by banks is the Swift system, which is a centralised approach. Should we be looking at a different approach?

Number of votes: 3

8. Guy has electronic key in his pocket, someone brushes into him and can eavesdrop/scan this key data. This is also happening with electronic locks on autos where criminals can use laptops to open cars.

Number of votes: 1

9. Making the mobile phone into a payment mechanism as trusted as the Visa credit card model.

Number of votes: 0

10. Television domain based services. Provision of enticing, configurable, customisable, mobile services to end users irrespective of the network (NEM philosophy) will foster EU competitiveness, diversity of language, multimedia provision, etc.

Number of votes: 0

4.5 Stream 2 Workshop results - Extended Summary

The following provides a consolidated summary of the results of the Working group in Stream 2. The complete details of the challenges elicited during the session can be found in the [Annex](#) to this report.

The Stream highlighted a large number of both societal and technological challenges for the medium and long term research and development to enable security and dependability in the areas of Mobile Software, Services and Information.

Some of the non-technological challenges included the (i) creation of new, or the modification of existing, laws and/or regulations or (ii) identification of a new legal and regulatory body to enable sanctions and enforcement abilities for security and dependability, preferably outside of the government sphere. There is also a need for the research and business experimentation, including real users involvement and input, to be carried out and tested in the funded projects. There was a discussion on the need for truly interdisciplinary FP7 RTD projects related (not just) to usability - societal and business driven, as opposed to just technical – that typically need to be of long duration; because interdisciplinary research takes quite a while to become effective as the people from different disciplines learn to work together effectively.

A number of the technological challenges included the need to treat security and dependability more as a process, or even a service, with clearly defined specifications, which would assist in the

security and dependability awareness of the various stakeholders. This would enable all the experts and the users to be 'speaking the same language', or more specifically, consistent and comparable expectations. In addition, by specifying a process or service, traceability and responsibility could be placed. Specifications (clearly defined ones in particular) help to develop expectations about the intended behaviour of systems or services and, thus, allow all stakeholders to assess if their experiences match the specification. In positive cases, it raises the confidence that the system (in the future) may behave according to its specification. This fact may be called trust. As such, these experiences may change over time. To maintain the conformance of the technical system with its specification, on which stakeholders may rely, is in fact a process (or even a service). Security should not just appear as a cost but as a revenue source or an intangible benefit as well for some stakeholders. This is, of course, a greater challenge in the future with respect to the increasing dynamics of the technical systems and their services. For example, the design of mobile software and services including OSS design must include an up front security and dependability management specifications typically in UML 2. This would be part of a full service specification and would not be an add-on, as it is treated today.

There is a need to include the requirements of all of the stakeholders in the security and dependability of web services and software applications, including the end users, in the process. One of the long term challenges discussed was to replace the current (unjustifiably trusted) system creation environment with an end user based environment, which elicits their trust in a more proactive manner. This should be based on negotiation (or enforceable and sanctionable SLAs) between the end user and the provider in order to match the end user needs and their tolerable risk assessment criteria levels. This was considered a long term challenge because it cannot be done without revisiting, harmonising, changing and/or replacing the various approaches in use today. Currently, there is a lack of trust metrics to establish/define quality of trust and a well defined Standardised Trust Management model is needed with quantifiable metrics models for Security and Trust.

There were numerous discussions about an EU-based approach for digital rights management to enable the EU to become a more effective content creation and provision environment. In order to accomplish this to the benefit all of the stakeholders involved, it will be necessary to provide an framework and environment with protocols that will enable the traceability of the rights all the way back to the contents rights owner. There needs to be a proper balance between the rights of the producer, those of the supplier and the purchaser/user. Some of the technical approaches discussed included ontologies, asset identification, perceptual hashing and semantic linkages for traceability. These would have to cope with content that is changed throughout the whole chain ("who owns what and when") and the ability to observe the adherence to agreed rights. Best efforts must be made to enable transparency in rights distribution, and/or creation of DRM distribution networks. It was the strong feeling of the participants that if addressed within FP7, this could open up very new and exciting opportunities for special actors within this high growth potential area.

The elements required for an effective and economic certification environment were discussed. This would require an evolution of security metrics to determine the levels of security. Today, security services are either enabled or disabled and finer granularity is required. There is a need to increase certification level transparency. i.e. relate security increase to level increase and risk decrease --> economic impact of certification. Cross certification among different service providers e.g. via real time negotiation algorithm and dynamic certification with virtualisation for third parties based on trusted community is needed.

In addition to the original themes provided at the start of the workshop, the participants elected to contribute a number of other themes for discussion. These included the need to look at the Business Impact of having security and dependability, highlighting the associated economic losses, so as to wake up people without unnecessarily frightening and/or discouraging them. Security should be a business enabler and not a showstopper and we should be capable of correlating security impact with business impact in real time with advanced security analysis tools.

Another area of significant interest was the Grid security and dependability that need to be addressed to bring the Grid area into the ecommerce domain. It is recognised that Grid Security and Dependability is necessary before moving onto next step of content/data usage of Grids, which is the principle area of progression in FP7 for Grids.

A number of challenges were identified for the Risk management approach, which included the necessity for Models and best practices and automated tools, the need for Certification, threat identification databases, statistics of events (incidents), and the need for some 'formal methods' for its standardised evolution.

The need for significant research into the relevant legal and ethical issues is required for mobile computing (especially ambient intelligence, pervasive computing), an arena that is facing a serious resistance because of these issues.

With the general trend of outsourcing services to external companies/countries, we need to evaluate the 'impacts of outsourcing of security functionalities' also relative to the legal framework in which the outsourcing takes place. Outsourcing is creating a new business relationship that "intervenes" with an existing one, and, thus, the issues of data protections laws are in danger of being forgotten. They are very important and, therefore, the challenge is multidimensional and not only a technological one. Moreover, policy makers need to be exposed in projects to economic and social risks of R&D security.

Finally, there was also elaboration and discussions on the security and dependability requirements for Software Defined radio (SDR) including issues involving spectrum optimisation, the need for flexible services, certification of SDR platforms, local regulation on cryptography use, standardisation of SDR services and protocols, which are highly challenging because one has to balance the 'openness' and the 'controls'.

5 Working Stream 3 – Mobile perspective End User needs

Rapporteur: Keith Howker, Vodafone Group R&D

5.1 Executive Summary

Stream 3 did not restrict itself to consideration of only the end-user perspective of security and dependability, but also took into account a much broader interpretation of *user*, to include the many actors involved in delivering and supporting the envisaged ambient environment. The group returned constantly to the guiding questions: is it about mobile and wireless? does it require future R&D?

Three of the principal user concerns identified have many points of contact and overlaps: identity, privacy, and user empowerment. The common theme relates to users' requirements for appropriate control and visibility in matters that concern their personal, or their organisations', assets and sensitivities. This covers all aspects of information and communications services: from the simple voice call; to the complex high-value multi-party transaction; to profiles held by administrations or commercial enterprises.

With all these there is the enormous challenge how to achieve the proper balance between the rights of the individual and the needs of society.

The problems are generic in a converging ICT world, but the difficulties are that much greater in the heterogeneous, dynamic mobile and wireless environment with respect to providing technical solutions, management of the deployed technology, and the inclusion or the user and user preferences in the loop.

The other big area requiring further research is *trust*: how relationships between users and services (or other user) may be established, monitored, and maintained.

Accompanying this, is the general requirement for trustworthy services – from banking to health to environmental monitoring – and with it the need for the underlying security technologies to keep pace, delivering higher assurance and performance with lower cost and size.

Further research and development is indicated for the many technical issues, together with appropriate complementary work in the human sciences: sociology and psychology.

Stream 3 Participants

Giuseppe Bianchi
David-Olivier Jacquot-Chiffelle
Boris Dragovich
Stephan Engberg
Bernard Hämmerli
Mario Hoffmann
Keith Howker
Sabbah Jassim
Susana Jurado
Ralf Lindner
Simin Nadjm-Tehrani
Thomas Roessler
Thomas Kohler
Antonio Kung
Tobias Scherner
Alan Stanley

5.2 Stream 3 Overview

Introduction

The workshop was broken into three parallel *streams* that were to address three very rough divisions of the mobile and wireless landscape, together with a number of plenary sessions and presentations. Streams 1 and 2 between them addressed the hardware and software technological areas; Stream 3 set

out to look at the picture from the other side – from the user’s perspective – where the user is not only the end-user or ‘customer’ with the mobile terminal, but also the provider of services, the communications provider, the network operator and all the human hands involved in delivering and supporting the envisaged ambient environment. It came as something of a surprise that this was the most popular stream, even though the background orientation of the participants was still principally technological.

It is an ongoing problem to isolate what topics and areas require R&D work to bring about user adoption and satisfaction, and which aspects are more a matter of the industry recognising the opportunity or necessity to introduce the sorts of services that will fulfil users’ expectations. A further difficulty is to distil out of the general statement of requirements what is specific to the mobile and wireless environment, which is the actual question we are set.

Many issues would still be problematical in a fixed network/inter-network environment. The additional dimensions, firstly of wireless-ness, and then mobility itself greatly aggravate the difficulties, but they perhaps provide clearer focus on the challenges. New directions for wireless, such as *ad hoc* networking and relaying, bring further complication and uncertainty.

Many of the issues identified are about usability and human responses to technology which is fundamentally already available; the R&D component is therefore more about the psychological and sociological disciplines and their contribution to an overall strategy and design..

Full working results of Stream 3 Group may be found in Section 3 of the [Annex](#) to this report.

Principal themes and trends

User empowerment, privacy, and management of identity

Three of the principal user concerns identified have many points of contact and overlaps:. The common theme relates to users’ requirements for appropriate control and visibility in matters that concern their personal, or their organisations’, assets and sensitivities. This covers all aspects of information and communications services: from the simple voice call; to the complex high-value multi-party transaction; to profiles held by administrations or commercial enterprises.

Various partial ‘solutions’ are currently available that go some way to addressing each of these, but the issue requiring future research and development is an integrated approach that simultaneously delivers the necessary functionality and protection, together with appropriate assurances to the user. The problems are general

identity

not just the technical aspects of protection of user credentials, and how to achieve anonymity /pseudonymity - of user, user's actions, payments, etc., but the sociological and political issues and context; control of user’s identity, and all information relating to it, such as location, and preferences and profiles;

privacy

the requirement to retain control over sensitive information, owned by or relating to the user, whether released outside the user's own environment or supposedly still under its protection; plus specific issues about identity-related information, as above;

user empowerment

how to assign appropriate controls to the individual, as opposed to all controls being centralised in either major providers of choice – banks, Service Providers, etc.(discretionary), or monopolies – .gov, NHS, etc. where there is no choice.(mandatory); the issue is the general need for the user to be in control of its own information and resources, or rather the fear of not being in control: that, without the user’s awareness, let alone permission, commercial, governmental, or criminal agencies may gain unauthorised control or knowledge of the user, possibly by aggregating seemingly harmless fragments.

One may also include here concerns about legal interception

With all these there is the enormous challenge how to achieve the proper balance between the rights of the individual and the needs of society – the wish for *rights* to privacy and invisibility *versus* the need for accountability and *responsibility*.

Usability, Security, and Dependability

The next group of concerns relate to the usability, security, and dependability of applications and services accessible by the mobile user, together with those same aspects - usability, security, and dependability - of the actual communications media and channels. One may also include in this group the security-related services, functions, and interfaces, and the security of the mobile device itself.

Trusted device

A third group is about exploiting and extending the capabilities the mobile device to make aspects of our lives easier and more easily managed:

- generalised *access control device* – physical access, login, signature, etc.
- universal payment token and purse
- storage of and access to information – local caches and secure vaults: instant facts and figures as well as critical personal and health-related data.

The less popular scenario snapshots raise major concerns about the dynamic, heterogeneous ambient communications and services environment foreseen by the visionaries – seamless, secure, and dependable. Meanwhile how can the same ambience be exploited to contribute to the wellbeing of the planet and its occupants.

Trust

Two aspect of trust are identified:

- subjective – dependent on personal feeling or belief, supported by, say, reputation systems and frameworks;
- objective – based on assurances of verifiable trustworthiness of hardware or software functionality, including cryptography, trusted computing, security protocols, etc.

Questions arise about how trust is established, maintained, monitored and reported, and how charging and payment can be made trustworthy. Much technology is already available, accompanying work is required to provide human sciences/engineering support. The challenge is to establish a comprehensive framework for handling trusted relationships between all relevant entities, not just human users.

Anxieties

There were several common anxieties implicit in most of the issues, but mainly concerning the privacy-ID-empowerment constellation. These were about the increasing possibilities and opportunities for malicious or accidental misuse or disclosure of identity- or other sensitive information belonging to the user, and the user's lack of authority over it – *disempowerment*. The natural tendency would be for continuing centralisation of control, and with it an inability to prevent stealthy aggregation of the digitised user-portrait. A particular fear is the scope for wrong attribution of responsibility either by incorrect function or malevolent attribution of blame. A recurring matter was the possibility for naive, misplaced trust by authorities and others in biometrics in isolation, not in conjunction with other technologies – supporting, or supported by.

Conclusions

Tb be expected from the declared orientation of this group, the needs, rights and responsibilities of the human user are loudly and clearly articulated (even if not made fully apparent by this rapporteur). Complex concerns were voiced about the privacy, identities, and empowerment of the user; this was clearly top priority. Usability of the security facilities provided to the user, and the means exercising of user's rights and privileges, together with matters relating to trust and trustworthiness, was a strong second priority.

It may appear that the primary concern was security – where are the dependability issues? In fact dependability is implicit through out: the system and its provision of security measures is expected to

be usable, available, reliable, quick to recover, to say nothing of correct – in fact all the standard parameters of *dependable*.

A further area of concern relating to usability is the provision of effective levels of support for the user in form of contextual help, instruction and training, and design of correct procedures. These are required not only for the private individual, but the performer of a business role whether as an end-user of delivered functionality and services, or the provider, supporter, and manager of services and connectivity.

The fact is that all the issues raised do matter, and need to be addressed in future R&D. However, further analysis and consolidation is required in order to clarify what is called for in the FP7 workprogramme. Again, to be expected from the orientation of the group, the human issues form a significant sector of the whole R&D picture, and call for new research into the use and presentation of the technologies, whether they already available or are new in FP7.

5.3 Session Summaries

5.3.1 Session 1 – Scenarios

The purpose of Session 1 was to identify various scenarios – in the sense of *use-cases*¹ – providing or illustrating security and dependability issues that would require further work or study, and therefore could form a framework of topics and situations for discussion and investigation in the following sessions, as well as providing direct input to the overall workshop findings.

The process employed in the workshop to allow some parallelism within the Stream is described elsewhere [Section ****]. Even so, with the time allocated for this first session, it was never going to be feasible to work out developed scenarios based on extensive narratives. What we did produce was more about individual snapshots or specific aspects of envisaged usage which contained some interesting challenge or anticipated problem.

It would be possible to integrate some of these snapshots subsequently, and to develop more comprehensive scenarios that can be of use in the planning of FP7 workprogramme, and in the development of security and dependability specifics within the eMobility *Strategic Research Agenda* [SRA]

The complete list of issues raised in the session, together with a number of extended items generated during or after the workshop are given in Section **Error! Reference source not found.**, below.

5.3.2 Session 2 – Issues identification

Session 2 identified issues arising from the scenarios. The principle topics in terms of volume of input are outlined briefly here without seeking to group them. The full lists are available in Section **Error! Reference source not found.**, below.

Identity management

The need for granularity of accountability needs to be examined against the requirement for the user to adopt many identities and roles dependent on context and circumstances. The user should have appropriate control of management and use of IDs and ID-related information, including the possibility to revoke if appropriate. Attention was drawn to the risks arising from the possibility to link and to aggregate ID parameters to produce a larger identikit picture. Use of biometrics in identification and authentication should be restricted to a confirmation function, rather than providing fundamental mechanism due to current challenges from spoofing.

Privacy

Two aspects of privacy are identified: the basic concern about concealment of sensitive and ID-related information, including location; but also a more complex issue of the user's ability to retain some

¹ the alternative usage or understanding of **scenario** is not addressed here; that is the one mainly concerning *what-if* analyses of various possibilities and their outcomes, whether relating to business-cases, technologies, political, societal or economic developments, etc.

ongoing control over the use and propagation of information, including an ability to revoke or destroy <forget!>, and also to be provided with the ability to trace what happens to such information – who did what, where, and when? The issue of aggregation linkability arises again here – the ability to generate details of user actions and profiles [PIZZA] to the advantage of others and the possible disadvantage of the user. Can there be such an entity as a trusted privacy provider? The extent of local or cached information in the user's mobile equipment is questioned: on the one hand there is the wish for convenient instant access to a personal data-vault, but what are the consequences of loss or theft?

Protection of information in transit and while stored/handled is basic assumption. Protections should be context-dependent. The possibility of *trust-tags* is suggested. Traffic flow confidentiality should be available if appropriate.

Anti-fraud & local/legal interception

Suspicion was voiced about the scope for abuse of legal interception mechanisms supplied in good faith by connectivity providers (*vide* [Greek Watergate](#)): how to provide a technical platform that gives strict guarantees that the 'hooks' used for lawful interception cannot be exploited by other (unauthorised) entities than the ones meant to (authorised); can lawful interception be properly engineered, and not achieved at the expense of a threat to legitimate security needs.

Usability of security

Interfaces should be intuitive where possible. Continuity and seamlessness were seen as important qualities.

Particular emphasis is given to the needs of the naïve user, who must not allowed to be a danger to himself or to others. Safe defaults should be provided to the button-phobic. Users need to understand the impact of their actions. The possibility of a trusted intelligent proxy somewhere in the network was posited.

Security and trust status should be monitored and reported to the user in as well as moderating the action of the ME.

Compliance engineering

Two components were identified: the means of implementing trustworthy services and applications, and the means of verifying correct operation.

Training, awareness, and usability are essential.

The specific issue of verification of performance against a service contract or service level agreement is raised.

Service Level Agreements

There is a need for a dynamic SLA: both from the viewpoint of renegotiability, and also to provide for 'best available' performance in case of depleted resources due to emergency, say, in which case the user should only pay for delivered QoS. Options should be presented to allow conscious trade-off between security v. performance.

Trust

Questions arise about how trust is established, maintained, monitored and reported, and how charging and payment can be made trustworthy. Subjective and objective measures of trust are required. Is there a role for trust agencies or brokers, but how are the credentials of the broker established? in the same way as we trust our banks?

5.3.3 Session 3 – Issues consolidation

Session 3 examined priorities among the issues identified in Session 2. The principle priorities selected by the group are outlined briefly here. The full lists are available in Section **Error!**

Reference source not found., below.

Identity management

Further comprehensive study of requirements is foreseen in order to get the balance competing security needs of all parties involved. Basic priorities include decentralised, unlinkable, user-controlled ID management (i.e. pseudonyms; profiles; preferences; services histories, including the right to influence the routing of personal information and the right to delete/revoke/change data *globally*). Support for multiple identities is necessary – including anonymity and pseudonymity, required to preserve legitimate privacy, which should not be provided or controlled by a single management service.

Use of identity-related information should be strictly restricted to functional necessity. Use of biometrics should be restricted to confirmation role rather than being the prime factor.

Privacy and information protection

The top priority is seen as strict and enforceable restrictions on the external use and retention of personal information, whether sensitive (declared or from context) or identity-related.

Current attitudes are not to care about privacy until it is breached. Who is going to supervise, and how, the establishment of respect and value for personal privacy.

A technical challenge is how the user may retain control over personal information once it is outside immediate protection, including revocation, automatic time limits on use, and mandates to forget.

Anti-fraud & legal interception

The technical platform for legal interception should be strictly controlled and available only to warranted access, and not be exploitable by covert, unauthorised entities.

Usability [1] end-users, subscribers, users-of the system

Two aspects were treated separately, but there need be no distinction between the requirements of the end-user and those of the operator or systems engineer responsible for provision and maintenance of services. The whole topic is probably more to do with psychology and human interface design rather than underlying technology enablers.

In addition to the provision of the necessary technical interfaces, research is indicated into the design of the human interfaces and procedures, and the design and provision of contextual help and support, and preparatory instruction and training. The research challenge is what can users actually understand: of the interfaces and available instruction, but also of what is actually going on, and why – in particular, are critical situations recognisable to the combination of the system manager and his toolkit?

The needs of the naïve user must be given adequate priority.

Compliance engineering

There is a need for the verifiability of processes and tools for monitoring compliance. Many current vulnerabilities and breaches concern inadequate education and training. The ID issue of separation of functional role and personal accountability is essential here.

Transparent and flexible Service Level Agreements

The question is posed as to how to avoid discrimination against the end user, however equally important is how discrimination may be justifiably be made in order to ensure priority of essential aspects of infrastructure, during and emergency, say. The related issue is how to apportion resources to support some minimum guaranteed level of service in critical circumstances.

User empowerment

Research is required into a whole new perspective of responsibility and control. What are the legitimate needs of the user and what are the incentives and injunctions on the service provider? Investigation is required into scope – options, limits and feasibility – of the whole issue of citizen empowerment: social, economic, cultural, and technical issues

Trust

Research is required into what are the mechanisms that can signify credibility regarding trust, and measures of trust dependent on context.

They appear to be two separate areas: subjective trust based on reputation systems and personal assessment, and objective trust based on demonstrable qualities such as correctness and compliance.

Is there a necessity for (trusted) trust brokers – *cf.* banks – that guarantee service recommended providers, and accept, at some cost, liability for defaulters?