
**PROJECT FULL TITLE: F**acilitate **I**ndustry and **R**esearch in **E**urope

**GRANT AGREEMENT N.** 318762

DELIVERABLE D4.4

# Pan-cluster RTD workshops

Due Date : 28 02 2014
Main Author : NSMC
Contributors: ADS, AMETIC, CYBERNETICA, IFIS, LSEC
Dissemination : Public

# Document Control Sheet

| | |
|---|---|
| Project Number | **318762** |
| Project Acronym | **FIRE** |
| Work-package: | **WP4** |
| Last Version: | **1** |
| Issue Dates: | **28/02/2014** |

# Classification

This report is:

| | |
|---|---|
| Draft | |
| Final | X |
| Confidential | |
| Restricted | |
| Public | X |

| | |
|---|---|
| Partners Owning | NSMC |
| Main Editor | LSEC |
| Partners Contributed | All |

# Table of Contents

# 1 EXECUTIVE SUMMARY

The aim of this paper is to report on the workshops which were organized to validate the draft of Research Agenda in Trustworthy ICT, which will ultimately be updated to include recommendations for joint research and information exchange programmes at pan-cluster and EU level.

Five broad Research Themes have been used to discuss the topics of Research Agenda and research challenges. These themes are:

1. Establishing trustworthy relationships
2. Information privacy, assurance and cyber security
3. Addressing implications of trends in scale and complexity
4. Encouraging and supporting appropriate user behaviour
5. Proving fitness for purpose

The main outcomes include identification of new research topics, research topics which might be combined together and comments on the prioritization of the topics. In particular, 19 potential new topics were identified and the reviewers saw similarities between 8 of the existing topics. Most of the comments were related to topics covering Internet of Things, Hardware security, User empowered privacy, Information risk management and Big data.

A new Theme 6 “Cyber-Physical System Security” is proposed to capture comments by reviewers, and will be validated with stakeholders.

All the conclusions will be discussed with the members of the Industry and Commercial Networks or ICNs (End users) and Advisory Board to develop the final version of the FIRE Research Agenda which will provide input to the European Commission and other stakeholders developing roadmaps and strategic agendas for Trustworthy ICT.

# 2 INTRODUCTION

The aim of this paper is to report on the Pan-cluster RTD workshops which were organized to provide a validation of the draft Research Agenda (D4.2) in Trustworthy ICT from the perspective of each of the partner Member States.

A series of workshops was organized with a wide range of stakeholders to validate the draft Cluster Research Agenda and stimulate RTD collaboration between end-users (both small and large businesses), academic and other research bodies and the IT solution providers.

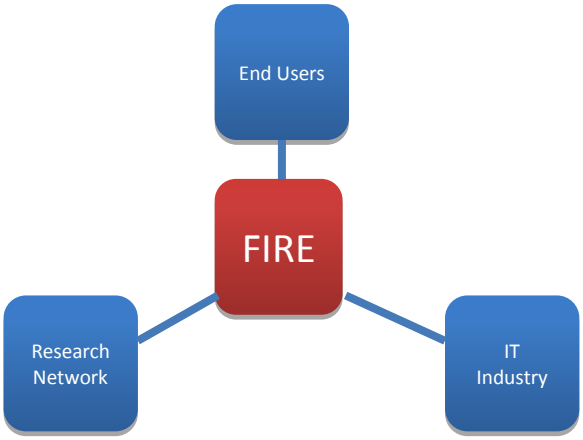


**Figure 1 - FIRE Stakeholders**

The workshops were organized nationally, and the concept was formulated by discussion within the Pan-Cluster Steering Group.

# 3 METHODOLOGY

## 3.1 Objectives of the Workshops

The main aim of the meetings was to validate, extend or amend the draft Research Agenda, D4.2 which formed the core of the discussion.

The main objectives of the workshops were:

- to validate, extend or amend the draft Research Agenda (D4.2) with a national perspective from each of the partner Member States
- to provide a forum for information exchange to identify, promote and share best practices and hence help to stimulate RTD collaboration between industry and the research community,

## 3.2 Type of Attendees

To validate the draft Research Agenda, it was recommended to use both consultation in plenary sessions and face-to-face meetings. For plenary sessions an audience comprising 6-20 delegates was targeted as more may have required additional resources to record the observations. They should include representatives from:

- Industry (end-users)
- IT security industry (including research)
- Research/Academia

It was recommended that the composition of the discussion groups should be balanced between these three groups.

There are three trans-national groups of participants contributing to the project:

- The Industry and Commercial Networks or ICNs (End users) covering Energy, Finance, e-Government, Health and Mobile Communications
- The Research Community (Industry and research organisations active in the field) contributing through a Research Network
- IT Security Industry (the FIRE Partners are working with current solution providers to capture their views)

Each partner represents a cluster of End Users, Research Organisations, and IT Security companies in their region, as follows:

- AMETIC: Spain
- LSEC: Belgium and Netherlands
- ADS: UK and Ireland
- IFIS: Germany
- NSMC: Czech Republic
- CYBERNETICA: Estonia and Baltic states

## 3.3 Framework of the Workshops

Each partner held its own RTD workshop or workshops, with participants from academia and industry. Each workshop had its own agenda and was reported to the task leader. It was deemed acceptable for the workshops to form part of some other event if that produced adequate access to participants.

The project FIRE and the Research Agenda were introduced in each workshop, followed by discussion between participants. To support the discussion of prioritisation of the Research Topics a hypothetical €1M for investment in each of 5 topics was used in some workshops to aid the ranking of the research Topics.

Each workshop was reported, using an agreed format.

The proposed structure of the RTD workshops report is:

1. Event Title
2. Venue and time
3. Agenda
4. Type and number of attendees
5. Methodology
6. Outcomes including feedback
7. Priorities of Research Topics (reported in Excel table, comments included)

### 3.3.1 Reviewing and Prioritizing the Research Topics

Firstly the draft Research Agenda was introduced. During the review process of the Research Agenda, reviewers were invited to consider themselves as investors and prioritise the Research Topics by investing a hypothetical €1M in each of 5 topics. The main method of capturing priorities was a set of A2 charts with one-line summaries of the research topics, grouped under the broad research themes identified by users listed below:

1. Establishing trustworthy relationships (topics 1-4)
2. Information privacy, assurance and cyber security (topics 5-15)
3. Addressing implications of trends in scale and complexity (topics 16-19)
4. Encouraging and supporting appropriate user behaviour (topics 20-21)
5. Proving fitness for purpose (topics 22-29)

Participants were given a brief verbal summary of how the topics had been identified and were then:

- Asked to review the topics
- Asked if any topic was missing
- Given five stickers each nominally worth a million Euros and asked where they would put extra investment to address what they saw as the most important research gaps

The following research topics, taken from the draft Research Agenda, were presented to the reviewers. These topics which have been identified by researchers themselves, are R&D challenges they have suggested, in response to the needs of users, to develop forward-looking techniques and methodologies that could improve the overall Trustworthy ICT landscape. This

list was not in order of priority, but identified suggested areas of research that address the main research themes emerging from the study.

**Establishing trustworthy relationships**

1) Dynamic Multiple-Identity Management.

2) Authentication of the Internet of Things (IOT).

3) Relating Trust to Information Quality.

4) Trust Models for Wireless Sensor Networks.

**Information privacy, assurance and cyber security**

5) Operational Assurance of Industrial Control Systems (including SCADA).

6) Industrial Control System Security and Hardware Security Solutions (including SCADA).

7) Thinking like an attacker.

8) User empowered privacy.

9) Socio-technical system resilience.

10) Incentivising information sharing on threats and attacks.

11) Resilience through Intrusion/ Compromise Tolerant Systems.

12) Modelling of Cyber-Criminal operations.

13) Secure computation by processing on encrypted data.

14) Post Quantum Cryptography for Secure Communications.

15) Post-process analysis of log data and security events.

**Addressing implications of trends in scale and complexity**

16) Value systems to achieve effective deep mining of 'Big Data'.

17) Understanding and countering Systems of Systems vulnerabilities.

18) System Engineering for trustworthy complex interconnected systems.

19) Protecting Privacy in a 'Big Data' world.

**Encouraging and supporting appropriate user behaviour**

20) Usable Security for Engineers and End Users.

21) Valuing Security Choices (Cyber Economics).

**Proving fitness for purpose**

22) Information Risk Management.

23) Automated Program Analysis and Verification.

24) Situational Awareness of Emergent Threats and Testing for Resilience against Future Threats.

25) Threat datasets for research to enhance security.

26) Secure and Agile Design.

27) Cross-Boundary Data Sharing Agreements for Data Centric Security.

28) Legal responsibility – rules for sufficiently securing ICT systems.

29) Assurance of systems (software, hardware and people).

### 3.3.2 General Recommendations

General recommendations were:

- To include a **moderator**, to help the discussion to be structured, meaningful and linked to the topic. As the audiences were composed of experts from different backgrounds, there may be a tendency for the experts to remain within their normal areas of competence, so the moderator had to ensure that the discussion stayed linked to the wider agenda topics. Moderators also needed to ensure that important and interesting ideas were not lost amid the pace and speed of the general debate.
- The use of a **Round table** is encouraged. The psychological benefit is immediately obvious to all; a round table is a place where everyone has the same position. This facilitates the mutual respect of other views and equally the right of each participant to express their own views.
- For purposes of smaller group discussion the introduction of a real or virtual **speaker's amulet** is recommended. The person with the amulet is the only one permitted to speak. This gives opportunity for an uninterrupted exposition of a view, while others need to wait to for their turn to respond until they hold the amulet. This helps with the debate of clear ideas and structured discussion in smaller, active groups of attendees.

The **audience** is the success key factor. In case of workshops associated with another conference, the profile of the participants is very important and should fit that of the required stakeholders. If the workshops were organized in the context of another event, one must be careful with the "open door" approach.

# 4 WORKSHOPS

Four partners organized workshops. AMETIC, ADS and IFIS presented FIRE and the Research Agenda at third-party events, while NSMC conducted its own workshop for this purpose. All of the workshops were held in December 2013. The workshops were organized nationally. The procedure of running the workshops differed slightly in terms of audience and local culture.

Five Research Themes had emerged from review of user needs and researcher comments on these needs:

1. Establishing trustworthy relationships
2. Information privacy, assurance and cyber security
3. Addressing implications of trends in scale and complexity
4. Encouraging and supporting appropriate user behaviour
5. Proving fitness for purpose

Using these grouped themes made it easier to discuss research topics, by providing a structure to which attendees could relate their views of research challenges.

Participants were asked:

- To review the topics
- To fill in the missing topics (if there are any)
- Where they would put extra investment to address what they saw as the most important research gaps using five stickers each nominally worth a million Euros.

## 4.1 Information day Workshop

AMETIC presented FIRE and the Trustworthy ICT Research Agenda in the following event:

- *Information day Horizon 2020 EU Framework Programme 2014/2015 Security research call (Madrid, 18th December 2013)*

Selected attendees of this event were contacted to provide them with information on the FIRE activities and outputs. Once information had been passed to them, they received a questionnaire regarding the research topics.

The main outcomes are described in the next section of this document.

## 4.2 ICT Security Research Meeting

The FIRE project and mainly the Trustworthy ICT Research Agenda were introduced at a specific workshop organized by NSMC partner. The event title was:

- *ICT Security Research Meeting, and has been held 5th December 2013, in Brno*.

The venue was close to the NSMC location, a neutral and independent area of hotel Kozák where there was a friendly and open atmosphere.

The workshop lasted 4 hours (17-21h). There were 25 attendees, representing 20 different companies and 2 universities. None of them was from the public sector; the IT industry was the main constituent (84% industry stakeholders, 16% academic). The attendees were selected from the ICT security industry and their participation was confirmed 3 days prior the event.

The main outcomes are described in the next section of this document.

## 4.3 Research and Innovation in Critical Infrastructures Workshop

IFIS presented the FIRE project and key elements of the proposed Research Agenda for Trustworthy ICT at the following event:

- "*Research and Innovation in Critical Infrastructures"*, (10th December 2013 in Aachen, Germany)

The workshop was hosted by STAWAG / E.V.A Group (Aachen), which was an advantage in providing logistics and inviting participants to this half-day event.

The majority of attendees had a professional background as practitioners in the Energy Industry RTD, so valuable feedback could be captured regarding the full scope of the topics presented. A strong emphasis of the discussion was put on research needs in the field of managing critical infrastructures, with a special focus on the role of security procedures and technologies.

The main outcomes are described in the next section of this document.

## 4.4 Academic Centres of Excellence in Cyber Security Research Conference Workshops

ADS attended two UK conferences involving relevant stakeholders for the Trustworthy ICT Research Agenda and ran workshops there. The first was:

- *Academic Centres of Excellence in Cyber Security Research Conference*[1] *– 3rd December 2013 – Solihull UK*

The Academic Centres of Excellence in Cyber Security Research Conference are organized by GCHQ and EPSRC. They brought together all 11 UK Academic Centres of Excellence in Cyber Security Research (ACEs), plus at least 10 other Universities that have relevant expertise and are candidates for future ACE status, and other key UK Government stakeholders such as the Cabinet Office, Department for Business Innovation and Skills, and Centre for the Protection of National Infrastructure (CPNI). A list of attendees was not published but the numbers totalled about 120 with approximate composition:

- 30 (25%) Public Sector
- 75 (63%) Academic
- 15 (12%) Industry

The main outcomes are described in the next section of this document.

## 4.5 Cyber Security Conference 2013 Workshops

ADS together with partner LSEC attended a UK conference involving relevant stakeholders for the Trustworthy ICT Research Agenda and ran workshops there.

- *Cyber Security Conference 2013 (CSC2013) – 9th December 2013 – Lancaster UK*

[1] For more details of the Academic Centres of Excellence go to:
http://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx

The Cyber Security Conference organized by the University of Lancaster, in partnership with the ICT Knowledge Transfer Network, explored the business opportunities related to the cyber security market with a focus on the Internet of Things (IoT) and Smart Cities. The event discussed how to ensure that UK businesses are ready to defend against these threats, and how they would also be able to take advantage of the gaps in the market place for new products and solutions to help protect others. Attendees (81 in total) covered all the main stakeholder sectors:

- 12 (15%) public sector
- 20 (25%) academic
- 2 (2%) large industry
- 47 (58%) SME

In both cases the workshop was held close to where participants met for networking and refreshments, allowing participants to participate when they chose. In the Lancaster Conference there was less time available for participants to visit the workshop and there were exhibits for them to see in parallel, which reduced the level of participation but increased the depth of discussion.

The main outcomes are described in the next section of this document.

# 5 MAIN OUTCOMES FOR RESEARCH AGENDA FOR TRUSTWORTHY ICT

## 5.1 New Topics Identification

The following research topics were indicated to potentially be missing by some of the reviewers. These topics are, in some cases, already included in the full definitions, which the reviewers may not have had time to read in detail. However, they may require further emphasis or a different articulation to bring out the useful comments made by the reviewers.

1. Cloud Security
2. Technical and legal mechanisms to protect data in the cloud.
3. Cloud solutions that include authentication and authorization solutions for persons, devices and machines.
4. Privacy in identity management, dealing with distributed attributes and identities.
5. User empowerment and privacy in the IAM area.
6. An M2M standard or industry-defined protocols that unite authentication systems.
7. Mobile Security
8. Cybersecurity simulation, scenario testing and training environments
9. Visual analytics and data mining for cybersecurity
10. Real-time risk assessment and management
11. Intentionality based risk analysis, this means making the risk analysis process take into account the motivation of the attacker to steal information or to break down the infrastructure.
12. Hardware based security approaches/ embedded security.
13. Supply chain security - cyber security of parts in the supply chain e.g. recycled IT parts (semiconductor components, etc.). Theme 5 – Proving Fitness for Purpose contains [26] Secure and Agile Design but the forensic provenance of hardware is also important.
14. Modelling environment development
15. Lessons from Biology
16. Techniques for analysing and understanding human factors issues related to cyber security
17. Public engagement on proportionate security.
18. Security in embedded systems is included in different topics, but it will be of greater importance in the future

In reviewing the topics some reviewers felt that there was a potentially important Theme missing. It was variously described but encompassed embedded, distributed systems whose primary functions were control and monitoring. Terms like cyber-physical, embedded, SCADA, ICS, IoT were used in trying to capture this idea. A new Theme 6 “Cyber-Physical System Security” is proposed to capture these ideas and will be validated with stakeholders.

## 5.2 Research Topics Which Might Be Combined

Attendees felt the following research topics were linked, and in some cases might be combined:

| | |
|---|---|
| **1 → 8**<br>**1 → 19** | 1) Dynamic Multiple-Identity Management and 8) User empowered privacy.<br>1) Dynamic Multiple-Identity Management and 19) Protecting Privacy in a 'Big Data' world. |
| **2 → 4** | 2) Authentication of the Internet of Things (IOT) could possibly overlap with topic 4) Trust Models for Wireless Sensor Networks, as the security can be seen as an intrusion tolerant network and the effort should be done on the network side. |
| **7 → 12** | 7) Thinking like an attacker – possible 'concertation' [joint action] across topics and 12) Modelling of Cyber-Criminal operations. |
| **8 → 19** | 8) User empowered privacy and 19) Protecting Privacy in a 'Big Data' world. |
| **10 → 13** | 10) Incentivising information sharing on threats and attacks could be an application for topic 13) Secure computation by processing on encrypted data. |
| **15 → 16,18, 19** | 15) Post-process analysis of log data and security events and 16) Value systems to achieve effective deep mining of 'Big Data' 18) System Engineering for trustworthy complex interconnected systems, 19) Protecting Privacy in a 'Big Data' world. |
| **16 → 21** | 21) Valuing Security Choices (Cyber Economics) is linked to 16) Value systems to achieve effective deep mining of 'Big Data'. |
| **23 → 28** | 28) Legal responsibility – rules for sufficiently securing ICT systems is linked to 23) Automated Program Analysis and Verification, if you regard the human as a threat to the system. |

## 5.3 Comments on Individual Research Topics

Attendees made comments on individual research topics as follows:

All research topics need an explanation of why this work is difficult, what the constraints are and what needs to be done. They should consider how this might be applied in the real world. Also, for example with topic 13, (Secure computation by processing on encrypted data) it would be helpful to make clear the maturity of the current research, e.g. in Technology Readiness Level (TRL) terms.

**1) Dynamic Multiple-Identity Management**. New approaches and activities close to innovation, including SME instruments, are needed, especially for BYOX paradigms.

**2) Authentication of the Internet of Things (IOT)**:

- Was identified as a "big topic". It extends to RF networks (note DDOS issue), Internet, and the Cloud. What is the range of cyber security risk over these domains and is the whole risk greater than the sum of the parts?
- User by host AND host by user: must be two way. Internet IPv6 which is the technology for IOT is ripe for abuse without two-way authentication: without a solution it will offer scope for new DOS attacks. Must include Machine-Machine as well as Human-Machine.
- Authentication will be the Achilles Heel in IOT

**3) Relating Trust to Information Quality**. There is a high risk that academic research will produce application specific models (which are less useful to users) as in the past.

**6) Industrial Control System Security & Hardware Security Solutions.**

- Endorsed but mixed views. Still have control systems using Windows NT which are vulnerable, but tools and methodologies already exist.
- Must obtain platform agnostic solutions that should be implemented in old low power and legacy systems.
- Hardware security is more mature, and thus less relevant from a R&D perspective, than other issues for Critical Infrastructure Protection (CIP).

**7) Thinking like an attacker.** Only support actions such as studies. This is not a research topic. Research on threat models is relevant to many fields, but is intrinsically covered by other topics.

**8) User empowered privacy**:

- Encumbering technology with privacy constraints has held up some security improvements. The return on investment has been poor.
- This topic has already been addressed and technically is very mature.
- User empowerment in the only solution for efficient privacy solutions.
- The EC legislation highlights the need for privacy-by-design technology.

**10) Incentivising information sharing on threats and attacks.** Not so much a research topic as an infrastructure or cultural need, perhaps supported via a new instrument or a Support Action. Cooperation, and thus information sharing, is fundamental for adequate protection of cyberspace.

**11) Resilience through Intrusion/ Compromise Tolerant Systems**:

- Growing importance, linked to Internet of Things (IOT). NPL in the UK is doing a lot of work measuring how data errors can build/ combine in an IOT system. The key question is when errors within parts of an IOT system pass through a threshold such that it becomes unreliable and you cannot use it and what effect a compromise has on the integrity of the system.
- What about tolerant in terms of availability and performance?

**13) Secure computation by processing on encrypted data.** Important to know where this topic has got to (in TRL terms): has it got beyond the stage of being computationally inefficient (and therefore not useful yet).

**14) Post Quantum Cryptography for Secure Communications.** One participant commented that in contrast to hardware advances there has not been a good advance in cryptography for a long time, and that what is needed is cryptography to much lower levels (cheap, low latency so does not affect data rate too much) that is enough to protect us against 99% of attacks rather than 1% of particularly sophisticated threats. Another saw this topic as contentious: it could be important or a waste of resource, depending on the definition of the topic, but properly posed it is an area of importance.

**16) Value systems to achieve effective deep mining of 'Big Data'.** Law Enforcement Agencies (LEAs) already work on this. Big Data analysis sheds a light on attack detection where

other technologies cannot. However, performance is still a limitation that needs to be addressed.

**17) Understanding and countering Systems of Systems vulnerabilities**:

- The stability of highly interdependent systems in systems of systems is not well understood.
- Need heuristic approach treating systems as entities plus work on provable security (this is what the system does, these are functions it performs, here are the consequences). This is often applied to products, sometimes components, but not systems as a whole.

**19) Protecting Privacy in a 'Big Data' world**:

- Particularly important for young people. However who should protect it? One participant was concerned this implies someone else does it for you. Users need to be in charge (Topic 8: User empowered privacy).
- Still needs legislative development before there is a clear context where technology can develop.

**20) Usable Security for Engineers and End Users.** Endorsed. Humans are fallible and users need usable and SIMPLE tools to manage their security.

**21) Valuing Security Choices (Cyber Economics).** Irrelevant to cybersecurity information sharing.

**22) Information Risk Management**:

- Manage the complex decision making process on technological risks based upon both the concept of the "potential profitability for the attacker", when someone takes advantage of a system weakness in order to commit fraud, and the potential impact (business, legal, reputational, social, etc.) of the security incident.
- Introduce intentionality as the backbone of risk management and orientate the decision making model on the analysis of the real situation, the profitability of the attacks and the existence of patterns of attack and defence.
- We need to move from traditional risk management to dynamic, real-time and automated risk management. We see this topic as being outdated.

**23) Automated Program Analysis and Verification.** We know code is full of holes and this is not improving. Most companies who write code don't have all the expertise they need and cannot buy it. We have good code for safety critical systems. Investment in this topic is important so programmers can write good software themselves.

**24) Situational Awareness of Emergent Threats and Testing for Resilience against Future Threats**:

- CIOs and IT Managers have to worry about Log Event data (which is Big Data in its own right). Web security, Email security, Firewalls, Mobile devices, Employment protection, switches…. and physically do not have time to read the data necessary to understand the situation. This is why services in security (Security Information and Event Management) are in the view of SMEs presently growing faster than product sales.

- Comprehensive identification and better understanding of the nature of cybersecurity hazards and their combined effects, and the development of new methods and technologies to prevent and address them, to mitigate their effects and to ease the recovery after an attack.

**25) Threat datasets for research to enhance security**:

- Difficult to understand the meaning of this topic
- One of the main problems in cybersecurity is the lack of complete and accurate datasets for technology validation purposes.

**26) Secure and Agile Design.** Since software is the main entrance point for attackers, any effort directed towards enhancing software reliability and security is worthwhile.

**29) Assurance of systems (software, hardware and people).** Address the assurance of data driven/ self-learning systems (that are stochastic in some way). The UK Research Institute in Science of Cyber Security (RISCS) Director recently stated that currently there is no way to quantify an organisation's security precisely enough to make it possible to judge whether it is more or less secure than before new security measures were implemented.

## 5.4 Research Topics with Lower Priority

Some individual attendees felt the following research topics should have lower priority:

6) Industrial Control System Security & Hardware Security Solutions. This should be the responsibility of companies not EU/ Governments.
9) Socio-technical system resilience. Wrapped up in other topics e.g. 11) Resilience through Intrusion/ Compromise Tolerant Systems.
10) Incentivising information sharing on threats and attacks. This already happens (in their view). Incentives are important but this is happening – needs business drive.
12) Modelling of Cyber-Criminal operations. Comes out of investigations.

## 5.5 R&D challenges Scores

During the review process reviewers were invited to consider themselves as investors and prioritise the Research Topics by investing a hypothetical €1M in each of 5 topics. The aggregated results across all workshops' reviewers, averaging the number of votes cast by the participants (the 70 who voted) for each Research Topic, show some interesting priorities which are summarised in Table 1.

| Theme No. | Topic No. | Topic Description | Average Votes per participant (70 participants voted) |
|---|---|---|---|
| 3 | 19 | Protecting Privacy in a 'Big Data' world | 0.39 |
| 2 | 8 | User empowered privacy | 0.27 |
| 5 | 29 | Assurance of systems (software, hardware and people) | 0.24 |
| 1 | 2 | Authentication of the Internet of Things (IOT) | 0.23 |
| 3 | 17 | Understanding and countering Systems of Systems vulnerabilities | 0.23 |
| 2 | 10 | Incentivising information sharing on threats and attacks | 0.19 |
| 2 | 13 | Secure computation by processing on encrypted data | 0.19 |
| 4 | 20 | Usable Security for Engineers and End Users | 0.17 |
| 1 | 1 | Dynamic Multiple-Identity Management | 0.16 |
| 2 | 7 | Thinking like an attacker – possible 'concertation' across topics | 0.16 |
| 5 | 23 | Automated Program Analysis and Verification | 0.16 |
| 2 | 6 | Industrial Control System Security & Hardware Security Solutions | 0.14 |
| 2 | 9 | Socio-technical system resilience | 0.14 |
| 2 | 5 | Operational Assurance of Industrial Control Systems | 0.13 |
| 4 | 21 | Valuing Security Choices (Cyber Economics) | 0.13 |
| 5 | 24 | Testing for Resilience against Future Threats | 0.13 |
| 5 | 28 | Legal responsibility – rules for sufficiently securing ICT systems | 0.13 |
| 3 | 16 | Value systems to achieve effective deep mining of 'Big Data' | 0.11 |
| 5 | 26 | Secure and Agile Design | 0.11 |
| 2 | 11 | Resilience through Intrusion/ Compromise Tolerant Systems | 0.10 |
| 2 | 14 | Post Quantum Cryptography for Secure Communications | 0.10 |
| 1 | 4 | Trust Models for Wireless Sensor Networks | 0.09 |
| 2 | 12 | Modelling of Cyber-Criminal operations | 0.09 |
| 3 | 18 | System Engineering for trustworthy complex interconnected systems | 0.09 |
| 5 | 25 | Provision of threat datasets for research to enhance security | 0.09 |
| 5 | 27 | Cross-Boundary Data Sharing Agreements to improve Compliance | 0.09 |
| 5 | 22 | Information Risk Management | 0.07 |
| 1 | 3 | Relating Trust to Information Quality | 0.04 |
| 2 | 15 | Post-process analysis of log data and security events | 0.04 |

**Table 1 - Workshops' view of research priorities**

If one groups the topics into the five Research Themes:

1. Establishing trustworthy relationships
2. Information privacy, assurance and cyber security
3. Addressing implications of trends in scale and complexity
4. Encouraging and supporting appropriate user behaviour
5. Proving fitness for purpose

The Themes with higher numbers of topics tend to attract more participant support because they give more opportunities to attract votes, which makes it harder to draw conclusions. It is more useful to look at how important stakeholders regard the topics within each Theme: if one looks at the Top 10 Research Topics from Table 1 four of those topics are from the Information privacy, assurance and cyber security Theme which appears to be the highest priority from these stakeholders point of view. See Table 2 below.

| Theme No. | Research Theme | Average Votes per participant for each Theme | Number of Research Topics in Top 10 |
|---|---|---|---|
| **1** | Establishing trustworthy relationships (4 topics) | 0.5 | 2 |
| **2** | Information privacy, assurance and cyber security (11 topics) | 1.5 | 4 |
| **3** | Addressing implications of trends in scales and complexity (4 topics) | 0.8 | 2 |
| **4** | Encouraging and supporting appropriate user behaviour (2 topics) | 0.3 | 1 |
| **5** | Proving fitness for purpose (8 topics) | 1 | 1 |

**Table 2- Relative priority of Research Themes**

The partner workshops in the Member States were generally consistent in prioritising:

- Protecting Privacy in a 'Big Data' world
- Authentication of the Internet of Things (IOT)
- Usable Security for Engineers and End Users

as important research needs (all appeared in their Top 10 research topics), but other priorities varied by Member State.

In the UK the following ten topics were ranked most highly:

- Protecting Privacy in a 'Big Data' world
- Understanding and countering Systems of Systems vulnerabilities
- User empowered privacy
- Authentication of the Internet of Things (IOT)
- Assurance of systems (software, hardware and people)
- Automated Program Analysis and Verification
- Secure computation by processing on encrypted data
- Usable Security for Engineers and End Users
- Industrial Control System Security & Hardware Security Solutions
- Valuing Security Choices (Cyber Economics)

In Spain the top ten topics were:

- Industrial Control System Security & Hardware Security Solutions
- Resilience through Intrusion/ Compromise Tolerant Systems
- Authentication of the Internet of Things (IOT)
- Operational Assurance of Industrial Control Systems
- Testing for Resilience against Future Threats
- Protecting Privacy in a 'Big Data' world

- Usable Security for Engineers and End Users
- Secure and Agile Design
- System Engineering for trustworthy complex interconnected systems
- Legal responsibility – rules for sufficiently securing ICT systems

In the Czech Republic the top ten topics were:

- Protecting Privacy in a 'Big Data' world
- User empowered privacy
- Incentivising information sharing on threats and attacks
- Assurance of systems (software, hardware and people)
- Authentication of the Internet of Things (IOT)
- Dynamic Multiple-Identity Management
- Thinking like an attacker – possible 'concertation' [joint action] across topics
- Socio-technical system resilience
- Secure computation by processing on encrypted data
- Usable Security for Engineers and End Users

# 6 CONCLUSIONS AND NEXT STEPS

## 6.1 Conclusions

The Research Agenda has been validated by over 200 stakeholders, drawn from users, suppliers and the research community at 5 different workshops in 4 Member States.

The partner workshops in the Member States were generally consistent in prioritising:

- Protecting Privacy in a 'Big Data' world
- Authentication of the Internet of Things (IOT)
- Usable Security for Engineers and End Users

as important research needs (all appeared in their Top 10 Research Topics), but other priorities varied by Member State.

Four of the Top 10 Research Topics are from the 'Information privacy, assurance and cyber security' Research Theme which appeared to be the highest priority Theme from the workshop stakeholder's point of view.

In reviewing the Topics, the related topics of 'Big Data' and 'Cloud Services', their securing and processing and storage, together with legislative development, were highlighted. These topics seem to be covering part of many other topics such as Dynamic Multiple-Identity Management**,** User empowered privacy and Post-process analysis of log data and security events.

Some reviewers also felt that there was a potentially important Theme missing. It was variously described but encompassed embedded, distributed systems whose primary functions were control and monitoring. Terms like cyber-physical, embedded, SCADA, ICS, IoT were used in trying to capture this idea. A new Theme 6 "Cyber-Physical System Security" is proposed to capture these ideas and will be validated with stakeholders.

Many of the topics suggested for adding are, in fact, already considered but the reviewers comments will be taken into account with further emphasis on the suggested topics.

## 6.2 Next Steps

All the conclusions will be further discussed with the members of Industry and Commercial Networks or ICNs (End users) covering Energy, Finance, e-Government, Health and Mobile Communications and the Advisory Board to develop the final version of Research Agenda D4.3 which will be disseminated by work package 7.

# 7 ANNEX A

Photographs are shown below from the ADS and NSMC workshops.