



Public Consultation

Recommendations Questionnaire

Response by



WSAN4CIP: Wireless Sensor Networks for the Protection of Critical Infrastructures

<http://www.wsan4cip.eu/>

9 March 2010

Introduction

The Think-Trust project has identified an interim set of research challenges that require attention in order to provide trustworthy¹ hardware and software for the Information Society. These research challenges stem from the four priority areas identified in Recommendation 1 of the RISEPTIS Report (<http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>).

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

We are now seeking input on these interim research challenges from the wider trust and security communities. For further details on these research challenges, please see Deliverable 3.1B (Interim Recommendations Report) on the Think-Trust website (<http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html>).

If you would like to have your opinion heard, please score the identified research challenges in this questionnaire (pp. 3 - 11)

(Completion of this questionnaire should take no more than 15 minutes)

The feedback received during this public consultation process will contribute to the final Think-Trust Recommendations Report (D3.1C), due for publication in June, 2010.

Responses by Monday, March 1st, 2010

Paper: **Kieran Sullivan**
 TSSG
 ArcLabs Research and Innovation Centre
 Waterford Institute of Technology
 West Campus
 Carriganore
 Waterford
 IRELAND.

Electronic: consultation@think-trust.eu

¹ For the purposes of this questionnaire, trust and security covers a broad spectrum that includes the trusted use of (and trust in) communications and services; privacy and protection of personal and commercially sensitive information; and protection of services and infrastructure (cyberspace).

Questionnaire

Please assign one of the following scores to the challenges identified.

- A*** absolutely mandatory for progress from current position
- A** essential to provision of trust and security for Future Internet and the Information Society
- B** necessary to achieve broad usability and uptake
- C** required longer-term response to new technologies and potential threats
- D** required for provision of attractive and competitive services
- X** not necessary or not urgent

(optional)

RESPONDENT NAME	ORGANISATION	E-MAIL ADDRESS
Uwe Herzog, on behalf of WSAN4CIP project	Eurescom, WSAN4CIP project coordinator	herzog (at) eurescom.eu

	Comment	Score
1. Trust 'engineering'		
Development of overall <i>framework for trust</i>		
(a) Support trust relationships (establishment, management, and maintenance)		A
(b) Development, expression and use of trust indicators;		A
(c) Automatic computation of trust assertions, based on policy frameworks that take into account user preferences;		A
(d) Life-cycle management, including maintenance, repair and recovery;		A
(e) Models, methodologies, measurement of trust (see Quantification below);		A
(f) Tools to calculate it (a combination of assisting the user and quantifying personal trust);		B
(g) Assessment of availability / downtime / integrity / confidentiality to feed into trust models		C
(h) Delegation and acceptance of trust and privileges.	unclear	
Quantification of trust, security and privacy		
(i) Scaling results on trust experiments from the laboratory environment to the real worlds of the Future Internet?		B

	Comment	Score
(j) Generalisation of security predictions across different software components, programming languages, systems, environments?		A
(k) Collection and sharing of security-related data for experimental research		X
2. Architecture		
(a) Policy awareness and transparency as architectural properties		A
(b) Transparency support : monitoring; observability; logging, accessibility		A
(c) Consistency of security and trust facilities and mechanisms across layers and domains		A*
(d) Meta architecture –higher-level abstractions to help structure a global information security architecture?		A*
(e) Network and service architectures – scalability and interoperability of the current architecture consider service composition/aggregation)		B
(f) Damage control: domains, partitioning, compartmentalisation in (e.g.) Cloud environment, including dynamic service composition/aggregation		C
(g) Architectural standards (to support) <ul style="list-style-type: none"> • pre-conditions for interoperability; • verification of conformance requirements; • built-in emergency measures; • establish workable definitions concept (metadata, ontologies, etc.); • support for security policy management, including the ability to attach policy information to data. 		B
3. Cyber-security: Engineering and Technology		
(a) Techniques and mechanisms to provide protection, assurance and integrity		A
(b) Robustness, resilience, survivability		A
(c) Criteria and standards to support policy governance		A
(d) Interoperability, and platform independence		A
(e) Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies		A
(f) Security in environments with scarce resources		A*
(g) Support for legal policies and requirements		B
(h) Tools and technologies to support design and construction of future trusted environments and networks		A
4. Accountability		
(a) Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress		C

	Comment	Score
(b) Interoperable, robust accountability framework: that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution		B
(c) Consistent interpretation of security policy agreements; appropriate standards for protocols and interfaces, and for tools to enable compliant usage		D
(d) Traceability and accountability on global accountancy-type principles		D
(e) Territorialisation of (trace/log) information; local domain policies and management; restricted 'sharing' only with authorised participating domains		X
(f) Real-time, large-scale test-beds to generate confidence		A
(related)		
(g) Applicability to charging and payment		B
(h) Anonymous/pseudonymous charging and payment systems		A
(i) Anonymization or impersonation tools to produce untraceable, but trustworthy, valid sources/channels for eg, provision of economic, social, or health statistics		A
5. E-Identity		
(a) Common EU framework for identity and authentication		B
(b) Interoperability of/with alternative (and current) ID schemes		B
(c) Flexibility of choice of identity and ID-protection options/choices, including partial IDs and anonymity when appropriate		B
(d) Life-cycle management of IDs, with protection recovery from loss or failure		B
(e) Standardised linkages to related and dependent concepts (accountability, access-control, etc.)		B
(f) Claim-based approaches using novel and existing cryptographic protocols to eventually avoid ID architectures with a centralised components that everyone needs to trust		A
(g) Technology to support new business models for central, decentralised, and claim-based approaches		B
(h) Communication setup and routing that are identity-data-aware only as necessary for network functions, without making the related users identifiable or traceable	unclear	
6. Privacy		
(a) Minimisation of unintended acquisition of personal and other sensitive information		A*
(b) Fine granularity access control to identity-related information		C
(c) Further development of Privacy Enhancing Technologies (PETs); tools to check privacy assurance and tools to advance transparency regarding used data		A*

	Comment	Score
(d) Use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users		C
(e) Methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, including revocation/retraction		C
(f) Possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates		A
(g) Personal/communal collector of personal garbage/litter (or timed auto-self-destruct)		A
(h) Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy (see 5(h), above)		A
(i) Standardised techniques to assure privacy across the various internet layers, through to network level and maintaining consistent privacy across different environments		A*
(j) Tools and concepts for deleting data in the internet ("forgetting") – see (g), above		A*
7. Protection		
Related to Privacy, above, plus confidentiality and integrity for business/administrations		
(a) Protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications)		B
(b) Domains, partitioning, compartmentalisation, fire-breaks – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage		B
(c) Fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc		A
(d) Mutual authentication, with multiple devices (ideally, technology invariant)		B
(e) New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age		C
(f) Uses of eID and its components in protecting the interests of its subject (data protection, etc.)		A
8. Usability		
(a) Support for the individual user (user-centricity)		B
(b) Environment can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles, depending on levels of (user) trust (of environment)		A
(c) What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered		A

	Comment	Score
(d) What are the impacts and implications for the underlying mechanisms and functionality	unclear	
(e) Attention to user/system interaction: sympathetic user interfaces, but with advanced options		B
(f) Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile).		B
9. Management and Governance		
(a) Framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs		B
(b) Investigation of economic feasibility and possible alternatives		B
(c) Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions; at a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to <i>common law</i> and the support of small claims		A
(d) The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc.		A*
10. Socio-economic		
(a) Convergence and coordination of technology with other areas and disciplines, with parallel advances in non-technological areas		B
(b) Explore role of other areas of business/industry should be examined to learn how they handle security/risk-analysis, eg, can the insurance industry balance risk and cost for different categories of users? with formal certification of trustworthy products/services and the classification of users, and no-claims discounts, additional premiums for risky use, exclusions, etc	unclear	
(c) Analysis of economics and inertia in the market place – why has security and trust been undervalued? – but possibly need to approach via the cost of insecurity; and user-perception of value of trust and security versus goodies and add-ons		X
(d) Incorporation of EU legal framework, for all jurisdictions currently covered, together with new laws and regulatory measures as necessary		D
(e) Constant engineering vigilance about economic viability: is it more cost-effective to (generically) prevent a data breach or just address the consequent (case-by-case) damage after the event		A

	Comment	Score
(f) Exploration of market place and related drivers for eID management (and other security and protection) <ul style="list-style-type: none">- to place Identifying credentials on different platforms- user-choice of ID 'home- economic value of secondary usages		B

Overall coverage (free text)

- Are there additional topics that need to be added to the interim list above?
- What topics need to be amplified or extended?
- Should any topics be removed, down-graded, or postponed?

Context and Overall Landscape

Please indicate your assessment of the importance of the listed items below:

	Comment	Score
11. Trends		
(a) Increased, heterogeneous accessibility to converged information and services. (For example, ubiquitous, mobile access, very high bandwidth fixed networks and access)		A*
(b) Increasing volume of transactions, and even higher volume of traffic	unclear	
(c) Large growth of sensors and slave-labour devices (<i>Internet of Things</i>), taking over the management of routine operations in commerce, utilities, the environment, and law enforcement and security provision		A
(d) Increasing mobility of users (physical or virtual), seeking either continuous (mobile) or intermittent (nomadic) connection and access to information and services		A
(e) Convergence of types: voice, visual, entertainment, social and business services. (eg, <i>twitter.gov</i> , and 'official' blogs)		X
(f) <i>Nano to mega</i> computing and communication – from cheap, incoherent, tiny, low-resource entities in massive numbers handling the routine, to the gigantic cooperative high-resource super-grids addressing the difficult and complex		A
12. Existing threats, vulnerabilities, risks		
<i>defects and failure/damage opportunities of the current Internet</i>		
(a) Fragility – networks and end-systems are vulnerable to simple attack, with information easily accessed, destroyed, copied and stolen, or falsified		A
(b) Software subject to design, implementation and usage errors, (hardware is not faultless, but more easily verified during design)		A
(c) Domino effect across inter-dependent systems in the case of accidental malfunction and/or failure, and attack propagation		A*
(d) Unprotected networked data exchange, but also via external media		A
(e) Lack of user-awareness regarding their data, together with difficulties in understanding and availing of privacy-providing tools. the burden to the user in using these often complex tools hinders their acceptance and uptake		B?
(f) Basic usable security and trust facilities that enable the user to make informed choices or decisions		B
<i>some malicious specifics</i>		
(g) Fraud – breach of enterprise records/systems, stolen/captured credit card and bank details		A

	Comment	Score
(h) Intrusion – Trojans: key-logging; colonisation, ‘hacking’		A
(i) Impersonation through identification theft or failure		A
(j) <i>Phishing</i> etc. relying on deception (spoofing) of user		A
(k) Identity profiling from digital trails		A
(l) Unauthorised disclosure: ‘inside jobs’ (police, government agencies, etc. for press and private investigators)		A
(m) Malware – viruses, worms, etc., for vandalism or blackmail/ransom threats		A
(n) IPR abuse – unauthorised file sharing, plagiarism		A
(o) <i>Denial-of-service</i> attacks		A
Unjustified trust – use of the ‘open’ net for sensitive operations (own goals)		
(p) Defence-related – internet gateways to ‘secure’ systems		A
(q) Emergency services		A*
(r) Utilities management		A
(s) Health systems		A
(t) Financial/economic systems		A
13. New threats, vulnerabilities, risks		
(a) New architectures will include structures and protocols that blur boundaries between: <ul style="list-style-type: none"> • what previously would be identifiable as domains (of, say, responsibility or control); • real, logical, and virtual domains; • where functionality actually lies – in hardware, in software, in the network, in information itself; • what is an application and what is a service 	unclear	
(b) need for new architecture (as a whole) to pay attention to its <i>own</i> security needs and implications, as well as those of its <i>clients</i>		A
(c) vulnerabilities from the increasing integration of services, and avalanching failure		A*
(d) total penetration of our lives, and consequent danger of the diminution and dilution of personal privacy and sovereignty (and that of enterprises or even administrations)		A
(e) the possibility of multiple <i>big-brothers</i> watching, recording, and analysing our actions		A*
(f) need for non-expert user to be informed, and to make appropriate decisions – in many cases, < I ACCEPT > the informed default advice from the “security” interface		B
14. FIA directions		
(the following are ‘givens’, but state your ranking in any case)		
(a) Management and Service-aware Networking Architectures		A
(b) Services and Software (platforms and infrastructures)		B
(c) Content Creation and Media Delivery		X

	Comment	Score
(d) Trust and Identity		A
(e) Internet of Things		A
(f) Real world Internet		A
(g) Future Internet Research and Experimentation		A
(h) Future Internet Socio-Economics		B

Annex: Further Reading

Please see Think-Trust Deliverable **D3.1B Recommendations Report (Interim)** for background information on this questionnaire. The Deliverable is available on the Think-Trust website:

[Click here](#)

(<http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html>)