"Security, Privacy and Trust in the Future Internet"
Issues for discussion

I. Introduction and General Considerations

The Information Society has become a reality with polymorphic fixed and wireless broadband networks deployed almost pervasively. Together with emerging service oriented architectures, they facilitate the composition and provision of interactive and personalised services and drive participative web technologies and web communities.

The inter-relationships and inter-dependencies between formerly stand-alone systems and networks are leading to complexities in the infrastructures of our society that have never been seen before. These complex systems and networks disseminate and process massive amounts of personal and business data, information and content in ways which are difficult to understand and control for users, in particular private citizens. In recent years we have witnessed a growing series of accidents and attacks on the Internet and on applications and databases. Through denial of service attacks, viruses, phishing, spyware and other malware, criminals disrupt service provisioning and steal personal or confidential business data for financial gain or other purposes. An increasingly organised and efficient though disruptive e-market is thus taking shape on an international scale.

Massive data gathering on individual behaviour for surveillance and service personalisation (though packaged as "enhanced functionality") may lead to the erosion of civil liberties through loss of privacy and personal freedom. These negative developments threaten to undermine the potential highly beneficial opportunities of the Future Internet.

II. Towards The Future Internet

In the last few years, a key debate has started on the ability of the current Internet to cope with the above security and privacy challenges together with other major emerging trends, notably: dealing with generalised mobility and scalability in the number of users, devices and services; and reliably delivering ever more time-critical and high-bandwidth applications. Research initiatives have therefore been launched in Europe and other industrialised countries on the design and development principles of the ***Future Internet***. This term encompasses, in fact, the emergence of future large heterogeneous and interconnected networked ICT infrastructures, as for example: the future evolution of the current Internet, the Internet of "Things", future wireless and mobile systems and sensor/actuator networks (post-IP, post 3G), mixed-mode environments consisting of diverse computing, communication and storage capacities, and service-centric, evolving and adaptive ambient environments[1]. It also encompasses the emergence of millions of different networked virtual constructs and entities. Examples here include enriched, dynamically evolving overlaid infrastructures (like virtual private or overlay networks, dynamic service software coalitions and interconnects, semantic P2P grids, etc.) and "virtual worlds" based on highly-distributed, virtualised communication, computing and storage resources.

III. Research Challenges

In this paper we address research challenges for the Future Internet from the viewpoint of security, dependability, privacy and trust.

[1] In other terms, the Future Internet is to be seen as an agglomerate of thousands of smaller interconnected systems and networks that are not necessarily interoperable, but open (i.e., with known interfaces) and possibly having their own proprietary protocols, as well as of trillions of heterogeneous networked computing, communication and storage devices.

Two overarching challenges could be identified:

- The creation of a trustworthy and resilient Future Internet as a conglomerate of networks and systems, with built-in security, dependability, privacy and trust.

- Enabling users to understand security, privacy and trust in the Future Internet by providing usable and credible support protecting their data and privacy. Thus enabling them to make informed decisions on the trustworthiness of information, services, social contacts and services.

The cross-cutting nature of the area of Trust and Security leads to consider three perspectives:

III.1 Securing the Future Internet

Many early network protocols that are now part of the Internet were designed for performance and not with explicit consideration of security. For example, they lack inherent notions of "identity", "time", and "location" that could contribute to enhancing network security and user accountability and liability. The new security architectures, models and frameworks must address the vulnerabilities and threats emerging in the Future Internet. The security policies must be adequate for protecting infrastructures, composite applications and virtual entities which span across different countries and administrative domains and involve dozens of different stakeholders, each conforming to disparate legislation and/or having their own security policies.

Future Research challenges

New conceptual frameworks, technologies and tools are therefore needed for:

- Managing and protecting the "identity" of billions of networked persons, devices, "things", services and virtual entities connected in the Future Internet;
- Securing the interactions and interfaces between heterogeneous ICT systems and engineering scalable security policies across the Future Internet;
- Securing critical infrastructures that are interdependent and controlled through vulnerable networks;
- Designing scalable, dependable and resilient open systems and composite services;
- Assessing expected security, dependability and resilience properties at design stage or during dynamic evolution at runtime;
- Predicting, monitoring and managing dependable behaviour, evolution and adaptation to changing contexts, operating conditions, regulations or practices of use, while guaranteeing service level provision or best trade-off between conflicting factors based on business oriented risk analysis;
- Security of highly distributed virtual entities and trusted infrastructures based on virtualised communication, computing and storage resources;
- New crypto schemes both in the core networks, to cope with ever increasing data transfer rates (crypto at Gbits/sec or even Tbits/sec), and at network edges (crypto for tiny networked devices with scarce resources like tiny WSNs, PANs, or other networked "things"); cryptography in the quantum era.

The above challenges address either core dependability and security technologies needed to allow creation of a secure and trustworthy Future Internet, or technologies that need to be addressed in conjunction with those developed in other objectives of the FP7-ICT Challenge 1.

At the **Network level** we must address i.a.: new network architectures and communication protocols that incorporate security, user accountability and privacy-protection and that protect identities of "things", services, virtual entities; network security, supervision, management and control; virtualisation and secure management of resources.

At the **software and service level** we must work on secure and auditable service platforms and middleware; trustworthy end-to-end services; virtualisation and secure management of resources; taking account of application and domain specific needs.

Concerning **networked media** attention must be given to trustworthy content, security in mash-ups, or authentication and secure web browsing.

III.2 Protection against emerging threats and vulnerabilities

One of the major problems in the current Internet is the weak security at its end points, i.e., protecting the end-users, their interactions and transactions, and their devices, content and data against any malicious activity. This is mainly due to: the lack of proper user accountability mechanisms; vulnerabilities of end user devices; insufficient user security awareness; or lack of economic incentives for good security offerings.

In the Future Internet, we must stop the fast and unpredictable development of threats as we see it today. At the same time, we must provide solutions that will address new vulnerabilities emerging from increased user mobility and technology complexity, proliferation of mash-ups and user-created and shared content, new social networks and virtual "worlds" and other still unforeseen developments in the Future Internet. We must also enable the merging of the virtual (digital) world with that of real physical objects in a way that allows secure feeling and acting on reality.

Future Research Challenges

Further research efforts will be needed for:

- Continuous and real time assessing and managing the security level of systems, content and services;
- Early detecting, monitoring and countering attacks, intrusions, new forms of malicious code distribution or any other type of malicious behaviour; understanding and predicting the threat models and their evolutions and proactively developing new protection schemes;
- Protecting interconnected key infrastructures of modern life against intrusions, attacks and cascading effects;
- Cross-border, cross-organisational, scalable distributed collaborative security mechanisms, including mechanisms inspired from the bio-living world: collective as well as self-organising, self-healing and self-learning protection mechanisms.

The above challenges address mainly core security and dependability technologies needed to protect the Future Internet against emerging threats. The following issues are however strongly linked to and could benefit from technology developments addressed in other objectives of the FP7-ICT Challenge 1:

At the **network level**, architectures enabling resilience and self-healing properties, together with network management and control tools for assessing such properties. At the **service level**, architectures and frameworks enabling event-driven management and service system resilience. At the **Internet of Things** level, autonomously adapting networked "objects" to vulnerabilities and threats.

III.3 Sustaining Privacy and Trust in the Future Internet Society

In their daily digital interactions and in emerging internet applications such as collaborative scenarios, virtual communities and environments, individuals are leaving a life-long trail of personal data. Technological advances facilitate extensive data collection, unlimited storage and data merging. Through user profiling, they enable more personalised service provision, while at the same time they create the conditions for tracking and tracing people and surveying their activities. In the Future Internet new tools and policies must be developed that will provide user-centric identity management (users control "what, where, when, and to whom") and that protect life-long privacy of users and their personal entities.

Companies and individuals will increasingly rely upon and exchange information and content they find on the Future Internet. We must develop capabilities and services that allow us to deal with the trustworthiness of data, information and knowledge, or the people we meet virtually and companies we deal with. This will include certifying data provenance and managing and negotiating trust relationships adaptable to the level of security and privacy required by users in a given situation and context.

Future Research Challenges

Hence, further research is needed for:

- Understanding and developing privacy-friendly identity management schemes;
- Rethinking privacy and trust in future ambient environments (incl. networked sensor environments and the Internet of Things): new privacy models and information control paradigms; privacy enhancing technologies;
- New frameworks and reference architectures integrating fragmented approaches for managing personal information and for data sharing and exchange under users' control;
- Understanding how trust emerges and evolves, and the related notions of reputation formation, monitoring, evolution and management;
- Developing novel trustworthy and usable means, including trust services, that take account of the situation and context and help users make informed decisions about which information, services and systems they can trust;

The cross challenge aspects in above research issues are clear and for example relate to:

Creation of trusted **Software and Service infrastructures** and trust in dynamic service coalitions. Personal data and privacy protection in **Networked Media** such as virtual worlds and the 3D Internet. Protection of the personal sphere and privacy in future **Internet of Things** and ambient environments.

IV. Projects in this area

Integrated Projects

MASTER
PRIMELIFE
TAS3
TECOM

Specific Targeted Research Projects

AVANTSSAR
AWISSENET
INTERSECTION
PICOS
PRISM
SWIFT
WOMBAT

Networks of Excellence, Co-ordination Actions

eCRYPT II NoE
FORWARD CA
ThinkTrust CA