DRAFT Position Paper

Editors: Volkmar Lotz (SAP) Zeta Dooly (WIT), Nick Wainwright (HP), Michel Riguidel (ENST),

Theodore Zahariadis (Synelixis Solutions), Yves Paindaveine (EU)

Email: fiacaretakers@think-trust.eu

1. Executive summary

The Trust and Identity breakout session at Future Internet Assembly (FIA) in Madrid will focus on cross-domain challenges for future research. This position paper provides a vision that the Security, Trust, Identity and Privacy community has developed and presented to the other domains prior to FIA Madrid for validation. More specifically, the paper describes some R&D priorities identified within this community and attempts to establish cross-domain support in order to ensure that a comprehensive view of Trust and Identity requirements are considered within the FIA environment. Initially, it is a contextual document that accompanies a questionnaire, which invites projects that have signed up to the Bled Declaration to contribute. A subsequent version will be released prior to Madrid. The new version is intended to accommodate the projects' initial input and reaction to the questionnaire. It is envisaged that the FIA breakout session in Madrid will facilitate discussions, debates and further refinements of this roadmap with stakeholders across all domains, as Identity and Trust parameters have been acknowledged as pivotal to the success of a Future Internet(s).

The paper starts with an investigation into some general assumptions on the Future Internet and their security, trust, and privacy implications. These assumptions are supposed to be shared among the security, identity, privacy and trust community, and their consolidation is meant to be part of the ongoing discussion. From the stated implications on security and trust, a roadmap is drafted that, on a high level of abstraction, reflects the current state of the art and indicates mid-term and long-term need for research contribution as well as productisation. It aims to provide some identified priorities and to establish cross-domain support in order to ensure that a comprehensive view of Trust and Identity requirements are considered within the FIA environment.

2. Assumptions/considerations for a Future Internet

Considering the leaps in technology advancement in the last 20 years, it is hard to envisage the Future Internet environment after 20 years and to consider unambiguously the challenges and solutions imposed on trust, identity and security related topics. However, some general assumptions can be made (at least, the community is likely to agree on them). When discussing them, a number of challenges that need to be met can be straightforwardly identified. These considerations give the planned Trust and Identity session at FIA Madrid some context, and can also be the target of consolidation across the different streams.

Assumption 1:

The Future Internet **whilst still layered, will be augmented by a number of cross-cutting dependencies**, leading to an increased **complexity** and distributed responsibility. While a simplified interpretation of the IST Advisory Group (ISTAG) view on the Future Internet[1] would allow to distinguish between the following layers:

---

[1] Please refer to the presentation of Lutz Heuser, Vice President of SAP Research and Chief Development Architect at the FIA Bled conference, March 31, 2008

- network & devices
- fundamental services
- value-added or business services
- Service Delivery Platforms, and
- Applications, ecosystems, communities

recent developments should be considered including:

- Business-centric networks
- Grid and cloud computing
- Virtualization
- Business grids
- Service ecosystems
- Personal or home environments

These research areas introduce orthogonal structures and new cross-domain dependencies. For instance, business-centric networks introduce business context (out of applications or services) to the network layer for the purpose of optimizing load balancing.

From a security and trust perspective, the complexity of the structures and the increased degree of distribution introduce the need for identifying the contributions and responsibilities of the participating entities (both technical and organizational), as well as means for tracing system behavior for the purpose of accountability. In the Future Internet, we foresee that there will be a stronger requirement on providing traceability and identifying responsibilities, but we will also increased challenges to meet them. Providing advanced methods and techniques for assurance and trustworthiness[2] may compensate here. Since tracing system, service or user behavior might reveal sensitive information, requirements on privacy or IP protection need to be balanced against appropriate auditing and control mechanisms. Research is required to provide future technologies fully satisfying specific needs for control and accountability with a minimum impact on privacy.

Assumption 2:

The Future Internet exhibits a **multitude in scale** compared to the current Internet, mainly due to the vast extension in scope caused by the inclusion of a multitude of connected entities of different types:

- Individuals
- Devices and things
- Services (both in the technical and in the business sense)
- Virtual entities and organizations
- Contexts (both physical and logical)

This has an immediate impact on the schemes for identity management, since all these entities need to be referred to, but likely in a different context and with different attributes. Key questions include: "Do I, need to distinguish between types of entities, and if yes, how,?", "Which types of entities are facing which constraints (e.g., related to privacy,, IP protection, etc.), "Which attributes are relevant and need to be evaluated?". While some of the recent and upcoming Identity management schemes provide partial

---

[2] We use "trustworthiness" for the existence of proper evidence matching trust claims, and "assurance" for the demonstration to entities of the validity of properties of interest. Both may refer to the same type of evidence. [Definition to be discussed and consolidated]

answers to these questions, identity for non-human entities and scalability of the approaches to the Future Internet remain challenging.

Assumption 3:

The Future Internet is likely to develop **spontaneous and emerging behavior and unanticipated new usages**. The history of the current Internet has demonstrated that much of its potential has not been anticipated, and there is no reason to conceive that this will be different for the Future Internet. The appearance of new entities, services and business scenarios will rather be the rule than the exception.

From a trust and identity perspective, the increased uncertainty resulting from new spontaneous and emerging behavior or new usage scenarios require advanced concepts for trust establishment and management. Much of the historical data ("historical" refer to previous observations of system behavior here) that current trust management systems rely on will not be available and trust might need to be (re-) established on different grounds (e.g.,, claims of properties certified by trusted parties. Means for controlling malicious behavior and unwanted usage become important to cope with the risk coming along with uncertainty. In addition, means to provide transparency and accountability as well as to assign responsibilities help to mitigate the risk while complex risk management frameworks may emerge as management tools.

Assumption 4:

The Future internet will be a **pervasive**, digital environment, composed of multiple interconnected **heterogeneous** infrastructures, terminals and technologies. This applies to infrastructure components and protocols, programming languages and concepts, as well as active content (e.g., scripting) and integration means (e.g., mash-ups, service composition environments). Heterogeneity in the networking and the terminal nodes will be thoroughly increased and nodes' capabilities will be further diversified (i.e. network interfaces & protocols, processing power, memory space). Powerful nodes will coexist with millions of tiny and nano sensors (even with the so called "smart dust") in an emerging "Real World Internet of Things". Machine-to-machine communication will be radically increased, leaving human-to-machine communication a small fraction of the network traffic.

As a result of the novelty and diversity of technology and their increased exposure in the scale and complexity of the Future Internet,, we will have to deal with a continuing stream of new vulnerabilities and emerging threats. The speed and the diversity of the technology development will make it difficult to respond timely to each particular vulnerability. Thus, we face a need for either generalized concepts or advanced predictive or responsive means (for instance, countermeasures for abstract threats or statistically based evolutionaru threat models)..

Assumption 5:

User-centricity and usability is a critical consideration and goal for the Future Internet. Users interact with the Future Internet (FI) throughout their lifetime, in varying roles, for instance, as private person, customer, business user, regulator, content "prosumer" (producer and consumer at the same time) etc., and in different communities and socio-economic contexts. Each of these situations imposes different identities, protection needs and trust requirements.

The majority of the users of the Future Internet are not supposed to be technical experts. However, users are, to some extent, aware of their protection needs within their universe of discourse[3] and their respective context. From a security and trust perspective, this asks for:

- End-to-end security
- Adaptive security based on rich context information, i.e. the system is aware of the user's situation and protection need and the related risk in the current system context.
- Understanding security, accountability, privacy and risk implications for the non-expert user
- The possibilities on the user side to be able to manage and choose different identities dependent on context, personal preferences or current roles

Assumption 6:

To a large extent, functionality in the Future Internet will be provided by means of services. Here, the notion of a service is used both in a technical meaning, as ubiquitously available infrastructure for integration across domains (as, for instance, Web Services do provide), and a business meaning, as service offerings can be leveraged through the Future Internet towards a new dimension of Business Ecosystems ("The Internet of Services"). Adaptive and flexible service orchestration, choreography and instrumentation will be the enabler for new and enriched businesses within and on top of the Future Internet.

For security, trust and identity, this puts a strong emphasis on decoupling related functionality from business functionality to overcome security and trust silos and provide the same level of flexibility as it is required from the business logic. With respect to identity, currently all or most services have their own ID management systems including storage of the personal data of their customers. This will become an insurmountable barrier to proper service innovation. We therefore will need to built an ID provisioning system that will be independent from the services itself, but directly usable by them in a proper overall ID architecture in a service framework. Analogous principles need to be applied to trust establishment and management, and security. The emphasis is on decoupling and interoperability, since the existence of a diversity of technologies has to be accepted (cf. Assumption 4).

3. Draft Roadmap – route to the Future Internet

It is recommended that the roadmap for Trust and Identity in the Future Internet needs to take into account a number of assumptions as described in section 2 above. This draft roadmap considers a number of concepts represented as 'lanes'. Each lane attempts to address three levels, respectively: a) current state of the art (the "today" perspective), b) emerging trends (the mid-term perspective) c) the future vision. Additional refinements might be introduced later.. As the focus of the Second Future Internet Assembly (FIA) in Madrid is on lane 1, Trust and lane 2, Identity and Privacy, the caretakers have focused the contributions and consolidation on these, however, initial drafts for lanes 3 to 5 are contained in the Appendix. The caretakers envisage that there is scope to further develop this roadmap toward planning for the Third FIA in Prague, Spring 2009. Therefore, it should be noted that these 'lanes' are not intended to limit but instead focus and frame the context for discussions, in FIA Madrid and many overlaps in the discussions may emerge as concepts are often inter-connected and/or dependent.

---

[3] This has been clearly expressed, for instance, by a participant of the FIA Bled conference discussions, stating that one of his major requirements on the Future Internet would be "Don't touch my money".

These high-level concepts need to inform *all* the decisions on aspects, priorities, mechanisms, interdependencies. An important part of the discussion needs to be related to technologies solving or mitigating potential or perceived trade-offs occurring such as:

- Unlinkability vs. traceability
- Full anonymity vs. accountability
- Security vs. performance / flexibility

a. Lane 1: Trust

This roadmap attempts to build a research agenda on a trust platform for the future internet.

It is easy to see why trust has emerged as a common theme across many domains in FIA Bled and thus toward FIA Madrid. It has many implications for networks, citizens, businesses, security, privacy, identity and others. The major challenge perceived is that of **scale**: while trust in the current networked systems is to a large extent a relation between a small number of parties (or even bilateral), the FI asks for schemes that include millions or even **billions of highly heterogeneous entities**. This leap is a consequence of the fact that trusted interactions may occur on the level of individual services (Services stream), things (Real World Internet stream), and information (Content stream). Given this, trust **spans all layers of the FI**, including the layers of personal users and their connection to the FI. Dynamics of trust becomes important: for instance, if changes in a service choreography occur, how do they affect the overall trust evaluation, in particular, since some of these changes might not be visible on some layers or for some entities?

The trust considerations, and how to embed them in the FI, should be informed by first developing and agreeing models for attaining mass confidence in participation in the FI-based society and economy by

- delivering security,
- attaining trustworthiness by means of rigour, integrity, transparency and openness in, and the ease of obtaining restitution from, the control processes and accountability chains

There is a broad consensus among the stakeholders that transparency and accountability are essential principles of the FI. This is an immediate consequence of the multitude of stakeholders in the FI contributing to its trust with distributed ownership and potentially conflicting interests.

The following solutions may be applicable to trust challenges relative to the three aforementioned timescales::

Today: reputation systems, PKI-based trust schemes, trust management for small groups of virtual entities, …

Mid-term: EU-wide or global trust center(s), privacy-preserving access to empirical data, mechanisms to ascertain minimal disclosure.. privacy-preserving data mining, trust based on attestation of properties, …

Long-term: real-time response trust schemes coping with spontaneous behavior or reacting to events, transparency, accountability, privacy-preserving utilization of PII in business processes (this allows for similar business models as today while retaining the privacy of citizens)

b. Lane 2: Identity & Privacy

Identity is a fundamental concept for a trusted and trustworthy Future Internet. In the FI, Identity management no longer applies to individuals only, but **extends to services, devices, objects, and virtual entities**. However, adequate schemes need to understand the difference in nature and role of the entities involved. Since an individual's interaction with the FI spans a lifetime and involves many different roles, the need for an independent ID provisioning and management system that smoothly interacts with the different contexts and respects a user's privacy becomes evident.

The relation between identity and trust is complex: Identity requires trust in a plethora of entities: systems and platforms that are involved in transactions for provisioning identities; software being used; protocols for identity federation; parties that vouch for identities. Then identity is again used to establish trust into parties, devices, organizations etc. As identity is a component of building trust, perhaps we need to consider an identity layer or indeed utilize frameworks [ref: Kim Cameron's Laws of Identity]. In addition, an "unlinkability layer" might need to be considered – otherwise the frequently stated demand on 'privacy-friendly identity service provision' could turn out to be unachievable.

The FI will have much larger impact on individuals', businesses' and authorities' interaction among each other, both due to the increasing number and size of such interactions, as well as their traceability over a long time span. Increased surveillance and profiling capabilities, sensing of actions, exchange of information and availability of information to an increased number of parties ask for enforcement of usage control, with an impact on SW architecture and network as well as hardware structures (Trusted Computing, privacy-preserving computing, SW attestation, …)

There is much attention being placed on **privacy-friendly identity service provision** (systems based on claims whereby instead of performing identification you claim your entitlement to a service and you give the proof of it without disclaiming further identity attributes[4].

Identity

> **Today**: advanced identity schemes for individuals (e.g., supporting federation), attribute certificates, …

> **Mid-term**: advanced identity schemes (including openID, Cardspace, Liberty) deployed for restricted scenarios (e.g., specific businesses), protocol support in products, privacy-friendly identity service provision, eID functionality integrated in passports / ID cards (suited for qualified digital signature), user provisioning from legacy systems, interoperable schemes…

> Delegation schemes, e.g., to allow children or elderly in a legal way to interact in the information society, will become increasingly relevant once identity infrastructures will emerge and major parts of governmental processes will move towards electronic processes. This is related again to accountability as the delegation complicates matters.

> Life-time aspects of identity management

> **Long-term**: Unified identity provision and management for users, services, things; user control over identity, , …Allowing for anonymity while retaining accountability; otherwise, it will be hard to get adoption in many environments; advanced hardware tokens; ontology- based reasoning over

---

4 Such systems include: uprove, ident-x of IBM, credentica recently acquired by Microsoft, etc.
We expect input here from F5 projects PRIME, PRIMELIFE.

trust properties of Identity Providers; fully-user-centric schemes; key management issues solved; recovery from credential loss

Privacy

Today: Policy languages expressing users' requirements, privacy-preserving computation schemes for selected scenarios and functions, trusted computing modules available (but not largely used), …

Mid-term: policy enforcement / usage control (based on trusted computing), privacy-aware privacy policy agreement;

Long-term: "virtual trusted computing" based on cryptographic schemes (supporting platform-independent usage control), generalized usage control concepts (applying to individuals and businesses), on-line policy negotiation and adaptation (of both policies and technology),

Additional challenges come from cloud computing when the service provider runs their services on virtual machines (VMs) on physical machines in the cloud owned by other parties in different legal domains, and when the virtual machines may be migrated between computation services providers or just physical machines seamlessly. Challenges: protection requirements for PII must be (provably) enforced by the computation environment the VM is running in. This is related to the Security Lane.

Another long-term aspect is real-time compliance monitoring, both within or across service boundaries which can ensure detection of policy violations. Major challenges here are architecture (e.g., a monitoring interface for services) and security challenges on how to prevent attackers (e.g., insiders) from tampering with events and logs. This strongly relates to security also.

4. Milestones toward community consensus building

- ICT Event 2008 **-** 25-28 November 2008, Lyon, France, in the *Networking* track of ICT 2008, the following sessions relating to ICT security and trust will be organised:
    - *Societal and ICT perspectives: the impact of Trust, Security, Dependability, Privacy and Identity*, by the ICT FP7 coordination action *Think-Trust*;
    - *European networks and services infrastructures security assurance*, by the EUREKA project *BUGYO-BEYOND*;
    - *Privacy meets ICT Practice*, by the ICT FP7 project *Primelife*;
    - *Privacy, Identity Management and Dependability in Emerging ICT-based Interaction Scenarios: Trustworthy Fulfilment of Requirements beyond purely Technological Innovation*, by the ICT FP7 project *PICOS*;

- FIA Madrid – 9-10 December 2008, Trust & Identity session – input to other sessions
- ServiceWave2008- 10-13 December 2008, Madrid, Spain
- FIA Prague - Security session
- Workshop for Think-Trust working groups Feb 2009
- RISEPTIS report – Autumn 2009

Appendix: Towards a completion of the roadmap

In this appendix, you will find initial drafts for the lanes on security, trustworthiness and non-technical topics. Since the focus of the discussion towards the Madrid event has been on Trust and Identity & Privacy, contributions to these lanes are less evolved. Discussion and consolidation will be part of the preparation for the upcoming FIA event in Prague.

Lane 3: Security

The security considerations, and how to embed them in the FI, should be informed by first developing and agreeing models for

- assessing and managing risks,
- assessing and managing liabilities,
- accountability for actions and decisions that are under obligations
- managing information rights
- managing oversight and control, including at a state level

(Cf. the Bled issues paper for a detailed investigation into related security challenges.)

Many issues around **_security_** revolve around future-proofing against currently **_unknown threats and vulnerabilities._** The main issues around **_trust_** revolve around the **_scale_** challenges posed by the FI.

Today: security patterns and best practices, protocols, cryptography, security models, formal methods and models, …

Mid-term: secure composition of services, security services, adaptive security, security best-practices enforcement, security-aware model-driven development, risk analysis and management, security monitoring and alerting, efficiency and performance, crypto and protocols for Wireless Sensor Networks (WSN), scalable authorization schemes beyond RBAC and UCON

Long-term: end-to-end security "by default", security-aware languages, automated security configuration driven by end-user's needs, responsibility, evolutionary threat models, predictive threat models, self-organising and self-healing security mechanisms …

Within these top-level concepts of security and trust, lower-level concepts and mechanisms also have to be addressed. Only then can even lower-level considerations be addressed, such as metrics, languages, algorithms, certification schemes, addressing schemes etc.

Lane 4: Trustworthiness

There is a broad consensus among the stakeholders that assurance, transparency and accountability are essential principles of the FI. This is an immediate consequence of the multitude of stakeholders in the FI and leading to the more general concept of trustworthiness, that includes security, proper authentication and accreditation, privacy and data protection, reliability, usability and quality of service. This must be implemented with increasingly distributed ownership and potentially conflicting interests.

Today: certification schemes for product security, static analysis, monitoring schemes, complex event processing, …

Mid-term: cost-effective certification schemes supporting dynamic environments, complex security metrics and indicators, advanced code analysis, SW attestation, …

Long-term: real-time proof of S&T properties,

Formal verification techniques are relevant from today to the long-term perspective. FP7 project AVANTSSAR is into this and could contribute some thoughts here. There is no trustworthiness without formal verification of protocols/components/systems

Lane 5: **Non-technical topics, governance, regulations**

Governance relates to the concept of relating real-life political power and law enforcement of geo-political entities to the reality of the Future Internet. How can interoperability and openness be preserved whilst at the same time geopolitical entities can protects their inhabitants against aggression from inside and outside on the FI. Distributed control within one interoperable infrastructure, with international agreements will be needed to avoid uncontrollable activities of Cyber war and growth of organized crime.

It is clear that these equally important non technical topics cannot be addressed in isolation from the more technical topics described above. The establishment of linkages with the Socio-economics breakout session could provide more information here. In addition, some early work has already taken place to coordinate the technical and non technical experts from coverage areas to better coordinate their future activities and to provide recommendations to both Policy makers and those responsible for building of the EU Research agenda for Trustworthy ICTs.

Today: varying data protection regulations, IoT governance infrastructure, some activities started bringing together ICT RTD and eGovernment and other non-technical approaches, …

Mid-term: a new framework for Policy developments and consequent RTD approaches incorporating both the technology and non technology axes; harmonized data protection regulations within EU; incentives for the market technology players to consider more comprehensive (secure, private, trustworthy) solutions for citizens, …

Long-term: International strategies for globalization, which requires compliance with strongest data protection regulations whilst preserving European societal values, ...

There is no indication of FI impacts on Authorization methods. The scale and dynamic complexity of the FI environment and services require revision of how authorization rules have to be defined, managed and enforced.

Currently used RBAC approaches cannot face the scale and complexity of FI. Failure to properly face authorization issues can have huge impacts on security and privacy.