Trust and Security in the Future Internet: Setting the Context

Towards a vision and analysis of fundamental change areas, challenges and potential solutions as discussed at EFFECTSPLUS Clustering and Roadmapping Events

Nick Wainwright, Nick Papanikolaou (HP Labs)
Version 1.0 [5/27/2011]

Table of Contents

Table of Contents 1
Summary 2
1. Introduction 7
1.1. Overview 7
1.2. Methodology 7
2. The Changes That Are Shaping The Trust And Security Landscape 9
2.1. Changes for End-Users / Citizens 9
2.2. Changes in the Business World 10
2.3. Changes in Society and the Wider Economy 11
3. Towards A Vision Of Trust And Security In The Future Internet 13
3.1. A Vision for Users of the Future Internet 13
3.2. A Vision for the Enterprise 14
3.3. A Vision for Society and the Wider Economy 15
4. What are the Difficult Issues to Address in the Trust and Security Space? 17
4.1. Enabling and Empowering Individual Users 17
4.2. Developing Security Technologies for Businesses 18
4.3. Broader Challenges 20
5. Approaches And Potential Solutions For Trust And Security In The Future Internet 21
5.1. Empowering Users 21
5.2. Enabling Business 21
5.3. Broader Recommendations 23
6. Conclusions ..... **Error! Bookmark not defined.**

Executive Summary

Summary of Process

The initial materials for the trust and security roadmap were gathered at three meetings organised in Effectsplus: (a) the Open Communications Event (01/02/2011), (b) the Technical Cluster meeting (29/03/2011), and (c) the Technical Cluster meeting (04/07/2011). At each of these events, the WP4 participants, Nick Wainwright and Nick Papanikolaou (HP) organised dedicated roadmapping sessions to gather inputs and validate results from earlier sessions. The structure of the sessions involved a presentation of the community's view of trust and security, followed by an interactive discussion of core topics.

The results of our analysis were processed, written up and circulated in the European research community of trust and security projects. The final version was presented at the Future Internet Assembly in Poznan (24-28/10/2011).

Summary of Findings of the Trust and Security Roadmap

The trust and security research roadmap[1] was organised into four major headings, grouping together the different findings from the events mentioned in the previous section. The first part of the roadmap presents *changes* that the community believes will affect the trust and security requirements for the Future Internet. These changes include differences in the way end users will use the Internet, as well as differences in the way business will be conducted over the Internet; also, there will be significant changes in the way society relies on the Internet, and these have significant implications for trust and security technologies.

Changes that will affect end users include issues such as the following. Clearly there are increasing usage scenarios for the Internet, including many that were largely unforeseen; social networking is an example of a now widely used technology that has changed the way in which people communicate and share information. People's attitudes are rapidly evolving and perceptions about privacy are shifting – namely, people seem to be more comfortable sharing details of their lives online. The pervasiveness of the Internet in our lives is affecting the way we live, as we generate more and more data about our lives that is stored and processed online.

There are significant changes occurring now in the business world that are being brought about by developments in Internet technologies. We are moving towards a world of Internet-based services, with service providers finding more cost-effective ways to interact with suppliers as well as customers. Of course there are numerous risks that need to be managed

[1] Nick Wainwright, Nick Papanikolaou, *Trust and Security in the Future Internet: Setting the Context (Towards a vision and analysis of fundamental change areas, challenges and potential solutions as discussed at EFFECTSPLUS Clustering and Roadmapping Events).* Research Report, Effectsplus project (http://www.effectsplus.eu).

given the massive quantities of customer-sensitive data that are shared between suppliers and service providers, including concerns about intellectual property ownership.

Wider changes in Internet use and dependence that have a bearing on trust and security research and development include the following. Entire societies are dependent on critical national infrastructure (e.g. electricity distribution networks, telecommunications operators, transportation systems and financial services), and such infrastructure is becoming increasingly linked to the Internet (for reasons related to monitoring, communications and various cost savings). Such infrastructure is therefore becoming increasingly vulnerable to attack. As recent events have shown, including the discovery of the Stuxnet malware, cyberattacks can propagate even in systems that are not directly connected to the Internet. Increasingly sophisticated cyberattacks are likely to emerge, with the potential to wreak havoc if adequate detection and prevention mechanisms are not in place and updated regularly.

The second part of the roadmap presents a vision for the Future Internet from the trust and security perspective.

The participants at the workshop envisioned a Future Internet that gives its users more privacy, especially through appropriate and effective control over how personally identifiable information can be used and transmitted online, and in particular, an *accountable Future Internet,* such that users and service providers alike can be held responsible for illegal actions and possible violations of consent. We expect legislation to evolve, particularly in the area of data protection, to keep up with the new business opportunities that Internet technologies have to offer.

An essential part of the vision for the future is that enterprises will be able to rely on the security of the infrastructure of the Internet as a foundation on which they can build secure, composable services (namely, services that can be combined together while still satisfying the same security requirements they satisfy in isolation); this, in turn, will enable reliable, protected information sharing between businesses and services. For businesses, there will be better tools to understand and manage risk; this is essential as more data and business processes shift into the cloud.

Open challenges in trust and security are the next aspect covered in the roadmap; we summarise some of the most important here.

The first important challenge is helping users to stay safe online; this means making online security and privacy much more user-friendly; there will have to be a number of helpful defaults, namely options that are universally or widely agreed upon, so that users can avoid the arduous task of making detailed choices and carry on with their day-to-day use of the Internet.

Finding the right balance between security and usability is a core challenge, and we are all too aware that there is no perfect solution. Developing intuitive security settings or configuration options will require much research, particularly given that Future Internet systems will have to be equally usable by ICT illiterates as well as specialists. Security contexts will have to be represented in an understandable way, enabling situational awareness for users.

But the most obvious challenge here is designing security into systems in such a way that it is almost invisible – thus reducing the cognitive effort required of the user; today's ICT users are already experiencing cognitive overload from the number of passwords they need to remember for different websites and applications.

Clearly there is no widely accepted notion of online trust, and more research is required in developing trust anchors for users. This is a fundamental challenge for the Internet of the future, which requires reliable indicators of trust for business and government to be conducted safely online.

In order to raise more awareness of security and the potential threats that lurk in the online world, it will be necessary to continually educate users. Users will need to be aware of their options, of the dangers and consequences of not protecting one's privacy, of the tools and technologies that exist to protect one's digital assets.

There already is a proliferation of digital identities in today's Internet, as individuals experiment with different personas, or more often are forced to create separate identities with different websites and providers of online services. From a privacy point of view, it may well be desirable to keep certain identities separate; in practice there will be a number of situations in which the use of a single online identity is convenient and beneficial. The challenge for the future is to develop identity management systems that give individuals plenty of control over access to identity information, while at the same time being useful online.

How is identity management to be achieved on the multitude of devices that people use on a day-to-day basis? How will digital identities be linked to individual people? In fact, should they be? For users of services in the cloud, how will trust be established between service providers who have no prior business relationship? All these questions are fundamental to the challenge of developing suitable identity management for the Future Internet.

There is the challenge of developing suitable biometrics for linking physical and digital identities. Biometrics are the most obvious way of extracting information from one's physical identity, but to what extent will biometrics become socially acceptable?

Trust and security challenges for businesses include: helping businesses assess and make decisions about risk using models and intuitive tools; helping developers build security features directly into their products; and expressing and enforcing security policies.

On the socio-economic front, there are a number of issues that will shape the world of the Future Internet. There will be a multitude of stakeholders, and many different ways to interact with different languages and kinds of expertise; the challenges around internationalisation of online services and adaptation of user controls to cultural expectations (e.g. different cultures have different expectations of privacy; this should be reflected in the privacy controls made available by service providers). There will also be challenges in finding suitable business models and means of charging for Future Internet services, for example creating privacy-respecting advertising.

There will be an absolute need for businesses to take an integrated approach when developing Future Internet products and services, combining legal, societal, user, and business perspectives with technology.

There will be a deluge of data, and a plethora of devices for accessing data; how this will affect the way we operate as a society remains to be seen, but it will surely impact our social interactions, the speed with which business is conducted, and the cognitive load we experience on a daily basis. Whether we can trust the data we receive and the devices we use is a challenge of central importance.

The workshop participants identified some approaches to tackling some of the trust and security challenges in the Future Internet; the major ones are discussed next.

Developing universally accepted digital identifiers. We have seen that individuals' physical and digital lives are increasingly connected, that they are controlling more and more devices and desirous of the ability to customize their digital experience. Meeting the challenges of providing usable digital identities while providing an adequate degree of privacy will necessarily require much interdisciplinary work; we believe that there is much to be done on the development of acceptable digital identifiers. To address some of the above issues, there should be work on new schemas for digital identity and an acceptable legal definition of a digital ID.**Developing languages and tools for specifying secure software.** There needs to be work on developing languages and formalisms for expressing unambiguously privacy, security and trust requirements. Tool support for reasoning and understanding requirements is essential, and in particular we expect the following will be important:

- Security analysis tools integrated in software/service development environments
- Visual/graphical representation of security state for awareness and analysis
- Tools to investigate emergent properties (security, safety) of systems
- Tool support for secure system building - from the design and specification phase through to deployment and operations.

Other related aspects that should be considered include the following:

- Quantitative security analysis – defining suitable numerical metrics for comparing security aspects of systems and models easily
- Security- and privacy-aware service composition

Privacy-aware software development. As we have seen, it is fundamental for privacy to be maintained in Future Internet systems, and there should be ways for developers of FI products and services to take privacy considerations into account and enforce appropriate policies where necessary. Indeed, privacy concerns should be integrated into software development. Some of the technical aspects of privacy that should be addressed in the future include incorporating privacy-preserving identity management and provisioning systems into the very fabric of Future Internet, deploying machine readable privacy policies everywhere where personal identifiable information may be processed, developing means of privacy-respecting advertising, and developing privacy enhancing tools for social networks.

Software engineering techniques for implementing permanent and complete deletion of digital trails with guarantees will help to solve many privacy problems. Research on privacy homomorphisms and cryptographic algorithms for enterprise computing, especially for cloud computing, will help enhance the underlying security mechanisms of the Internet.

Cooperation on Issues of National Security. International collaboration on security matters will be essential, particularly as cybercrime transcends national barriers. One example of a useful collaboration in area of trust and security would be the establishment of a secure and trustworthy international data exchange system for tracking cyberthreats and cybercrimes. Another type of collaboration would involve international standardisation of security features – and to some extent this has happened already with the EU's Common Criteria.

Enhancement of Legislation to Accommodate Technological Developments. An important area of work is the adaptation of existing legislation to provide adequate security and privacy protections given developments in FI technology. There should be a technology-aware legal framework for data protection, and a legally accepted means of offering end users a single point of trust and responsibility. Although to some extent such means exist today, the Future Internet should provide mechanisms to support law enforcement digitally. One unusual solution for certain types of cybercrime could be the notion of "digital jail": a digital jail, in the sense defined by Mike Surridge (IT Innovation, Southampton, UK) is a way to temporarily penalise digital vandals by restricting their online activities for a fixed time period.

Research and Investment in Security Tools and Technology. Integrating cryptographic algorithms into the software development lifecycle so that they can be built into tools more easily will help suitably educated developers make more secure system designs and implementations. In order to cope with ever-changing threats, investing in adaptive, possibly biologically inspired security mechanisms will likely prove useful; that way security systems will evolve and respond more intelligently to new threats.

Consideration of Novel, Radical Approaches. The following are germs of ideas that are subject to further development, and we will not expand on the details in the current version of this document.

Disposable systems. One approach to building security into systems is to make cheap, single-use devices that can be disposed and not-reused (especially by attackers!). This can be seen as a generalisation of the one-time pad cryptosystem to entire system-on-a-chip boards.

Loosely coupled systems. Developing systems with loose coupling makes it possible for their components to be replaced/exchanged with minimal effort if a threat is present, and assists the task of achieving *separation of concerns* in design. Strong security features can be built into individual system components without the constant need to worry about dependencies with other components.

Clearly, a number of significant R&D topics and opportunities have been identified in the trust and security roadmap for Effectsplus. We believe that the roadmap's findings are significant and novel and compare favourably to similar visionary reports from the United States – including e.g. the PITAC report (President's Information Technology Advisory Committee, "Cyber Security: A Crisis of Prioritization", February 2005).

1. Introduction

This document captures the outcomes of the research roadmapping and project clustering events[2] held under the auspices of the European Union's EFFECTSPLUS support action[3], held in Brussels 29-30 March, 2011. The participants at these events were all representatives of European FP7 projects in the broad area of Trust and Security.

1.1. Overview

The objective here is to identify and discuss, for the timeframe 2010-2020, a number of core **challenges** and issues, as well as a shared **vision** of trust and security in the Future Internet. First we begin with a discussion of **changes** and trends in the field; the analysis concludes with consideration of approaches and potential **solutions** to some of the various challenges identified.

1.2. Methodology

The ideas presented in this document were elicited from participants at the above mentioned events directly, and then organised and carefully categorised for the purposes of this document – in particular:

1. This report is organised under four core headings (Changes/Vision/Challenges/Solutions and Research Needs[4]), all of which are interrelated and constitute a basis for understand the key directions of research in Trust and Security in the Future Internet, as relevant to the European Union's Framework 8 Programme which will run from 2015-2020.
2. Participants were asked to identify concrete ideas for each of these headings in a series of rounds; during each round the ideas were written on Post-It notes, gathered and grouped together for discussion. There were two separate groups of participants, namely, a Cluster for Systems and Networks projects, and a Cluster for Services and Cloud Computing, and the authors respectively chaired these two discussions.
3. The authors then assembled these ideas into a mindmap, using the XMind software[5]. The mindmap was carefully edited and related ideas grouped together.
4. A further analysis and write-up of these ideas was then undertaken, resulting in this document.

This is the first draft of this write-up. It will be circulated to workshop participants for further refinement and discussion, and to reach some consensus on the core conclusions.

---

[2] See http://www.effectsplus.eu/effectsplus-1st-technical-cluster-meeting-march-29th-30th-2011/

[3] See http://www.effectsplus.eu

[4] Following the approach adopted for the Future Internet Assembly research roadmap which was originally suggested by Hans Schaffers (ESoCE-Net)

[5] See http://www.xmind.net/

This document focuses specifically on aspects of Trust and Security Research in the European Framework Programmes; naturally this will feed into the Future Internet Assembly Research Roadmap for Future Internet, which will also comprise other key areas of Future Internet Research.

2. The Changes That Are Shaping The Trust And Security Landscape

Future research into Trustworthy ICT will be influenced by a wide range of factors that will occur in the period under consideration. We can group the various changes that we perceive as having an impact on the field under the following rubrics:

- Changes in the way end users (citizens) perceive the role of the Internet in their lives and use it on a day-to-day basis; this includes current perceptions and attitudes, as well as end users' expectations for the future
- Changes in the way business is conducted, and how different sectors are being affected by developments in technology
- Changes in the broader socio-economic landscape

2.1. Changes for End-Users / Citizens

Users' Attitudes Are Changing Constantly

As the Internet becomes more integral to the way we live our daily lives, end users are becoming increasingly aware of the dangers of making too much information available publicly. People's careers and personal lives can be severely affected if they do not consider carefully what information (including multimedia – photos, videos etc.) they make available about themselves in cyberspace. Certainly there is a trend towards increased privacy awareness, although attitudes towards privacy are changing significantly – for many, the level of privacy concern is decreasing. This raises some interesting questions about the role of privacy-enhancing technologies and privacy-related research in the future.

Users' Physical And Digital Lives Are Connecting Seamlessly

We are moving towards a world in which everything – from your mobile phone to your refrigerator – is connected to the Internet all the time. The world of work and personal life are getting more and more intertwined as people use the same devices to access all their data. There is a trend towards convergence – this time, not a convergence of devices into one all-capable device (e.g. the smartphone), but rather a convergence of one's previously disconnected personal, social, and professional lives; what is more, this convergence is not being met with much resistance, making it more and more socially acceptable to mix these together. Through the use of different online personas/identities, people are able to represent themselves as they wish – although they most often choose to make their digital selves reflect aspects of their real, physical selves as much as possible (particularly in social networking applications).

There is a trend towards adopting widespread use of sensors; these will of course generate data that is often quite personal, as it reflects aspects of one's day-to-day reality. It remains to be seen whether privacy issues can be addressed adequately in sensor networks, or

whether they will hinder further developments and restrict the reach of the so-called Internet of Things.

Users Are Controlling And Regularly Using More Devices

The devices that people use are getting smarter and smarter; this means that people have ever more computing power at their fingertips, and that devices (particularly mobile devices such as smart phones or tablets, as opposed to desktop or laptop computers) will be at the centre of a fully connected, always-on world.

There is a change in the number of devices that people consider acceptable – it is common for people to carry several devices for different purposes, even though convergence makes it possible to do almost everything on a smartphone. It remains to be seen whether true convergence will ever be achieved (one device for everything which is universally acceptable in terms of features and other parameters e.g. size).

Users Are Demanding The Ability To Personalise Products And Services

Personalisation/customisation is an expectation that people increasingly have as they become aware of the capabilities of the platforms and hardware they use. As devices and applications become an integral part of people's lives, people want to have the ability to add their own personal touch and to combine features, capabilities and services in ways that are convenient to them.

2.2. Changes in the Business World

We Are Moving Towards A World of Internet-Based Services

The constant and widespread availability of the Internet has made and continues to make possible the provision and sale of many services. In line with the trend towards customisation/personalisation, users are demanding ways to compose services together and tailor services to their needs. Services provided through the Internet are becoming increasingly diverse and heterogeneous, and there is an industry trend towards business software being delivered as a service (SaaS). There is a trend towards massive centralisation and interdependence driven by cheap cloud and composed services.

In addition it should be noted that there is a rise in the use of location-based services, which raises significant potential privacy issues. However, as mentioned previously, users' attitudes are constantly changing and it is becoming increasingly acceptable to share one's location publicly (cf. services such as FourSquare[6]).

[6] See https://foursquare.com/

The Scale Of The Internet Is Constantly Growing

There is no question that the scale of the Internet is growing, with an ever increasing number of devices that connect – these correspond to reachable nodes, which are numbering in the millions at present. There is increased stress and strain on the internet infrastructure, with many more users and much more traffic. There are also ever more applications being developed, and through the use of social networking and micro-blogging (cf. Twitter), their reach can grow massively in the space of a few hours.

There Is A Massive And Continual Increase In The Quantity Of Data That Needs To Be Processed

The rise in the amount of data captured and managed continues unabated. Data is generated not only by people/end-users, but by machines and sensors. Data includes raw data as well as multimedia, the difference being primarily one of size. There are many issues surrounding how such data can be stored, administered and protected from unauthorised access, particularly given the speedy rate at which it is being generated.

ICT innovation is largely data driven, with business models that rely wholly on data mining and analysis becoming increasingly common.

Critical Infrastructure Is Increasingly Subject To Sophisticated Attacks

Business-critical as well as governmental infrastructure are increasingly targeted by attackers. What is essential to note is that critical infrastructure is getting connected to the Internet as a matter of necessity. Of course this is not without issues – and it is absolutely key to ensure the protection of national infrastructure against cyberattacks.

2.3. Changes in Society and the Wider Economy

Massive Growth of Cyber Threats and Cybercrime

The massive growth in cyberattacks, malware, viruses and Trojans in recent years is undisputed, and not just for the purpose of accessing or damaging critical infrastructure. The average user is becoming increasingly aware of online dangers and it is no longer safe to browse without firewall and antivirus protection. We expect that digital crime will increase, spam and viruses in particular growing at an exponential rate. In general, there is increasing opportunity for attacks and potential for failures in internet systems.

Without suitable countermeasures, it is possible for attackers to move into trusted channels and obtain access to sensitive or private data. The spread of malware through USB sticks and similar channels means that even pieces of infrastructure that are not directly connected to the Internet can be infected.

Broader Societal Changes

Globalisation implies the eventual abolishment of traditional trade barriers and the development of an integrated global economy. As this process continues, some elements of national infrastructure for different nations may well need to be linked, and the Internet will play a central part in this. It could be that a major internet security incident with serious socio-economic impact happens before the general populace is alerted as to the importance of security measures and technology.

There are other societal changes that will have an impact on the way we use technology in our lives – for instance people are likely to have more and more nomadic lifestyles – teleworking and telelearning (or distance learning) are two trends that are indicative of this possibility.

3. Towards A Vision Of Trust And Security In The Future Internet

In this section we develop a vision for Trust and Security in the Future Internet, describing how it will enhance our lives and what new possibilities it will enable for average users as well as security experts and developers.

3.1. A Vision for Users of the Future Internet

First we consider how trust and security in the Future Internet will affect the average user, and what this user can expect in the future.

Users Will Have More Privacy Online

Users are already becoming increasingly aware of the dangers of sharing too much about themselves online; we envision a future in which users will not have to worry so much about privacy due to the widespread availability of powerful privacy controls.

There seems to be a social trend towards decreased privacy concern; this, however, may change dramatically over time as people demand more control over their online identities and reputation. In fact, as privacy-enhancing technologies are adopted more widely, and people become more aware of their options with regards to their personal data, they may concern themselves *more* about privacy. It remains to be seen how privacy concerns will be perceived in the future, but in any case it is clear that users should *not have to* worry as much about privacy, given that technologies and infrastructures can be put in place to give people more control over their data.

We envisage a future in which users are empowered over privacy and personal data, and they have basic rights in cyberspace (freedoms, privacy).

Also we expect that there will be new business models that respect individuals' privacy more (e.g. for advertising).

Users Will Have A Better Understanding Of Security And Privacy Risks

There is little doubt that the average user of the Future Internet will be much better educated than users of today are about security and privacy risks online. We envisage a future in which users will be aware of dangers and online risks, and will know how to practically mitigate them. We also expect that there will exist good tools and technical support enabling end users to understand the security and privacy implications of any online services they use. So there are two aspects of our vision:

- the average user will be well educated about security and privacy risks online
- systems will be designed to assist users understand and prevent security and privacy risks to their data

This implies that, for instance, "browsing will be safe". Users will be trained to have situational awareness and be better placed to determine where to place their trust.

3.2. A Vision for the Enterprise

Next we discuss how business will be affected by trust and security developments in the Future Internet.

We Will Be Able to Build Secure, Composable Services

Businesses will rely significantly on the deployment of online services, and these services will be expected to have good quality of service; they will also need to meet industrially accepted security requirements and provide privacy and trust guarantees to end-users. Furthermore, it will be possible for businesses to reliably compose services to form new ones, while having confidence in the security properties of the latter. It will often be in the dynamic composition of services that added value will be found, and we expect that an open market for such services will be created.

Businesses will also expect to profit from providing users with customisation/personalisation options; it will be essential to give users choices while ensuring security and privacy guarantees are maintained. Indeed any security breach or loss of privacy is likely to have a significant impact for business, and so careful monitoring of services and of the facilities on which they are run will be essential.

Developers Will Have Tools Which Help Them Build Secure Applications

As more and more businesses rely on software and service development for Future Internet, there will be a fundamental need for compilers and development environments that assist developers in detecting and preventing security flaws and leaks in software. There will have to be good tools for software designers to understand and express security and privacy requirements. Furthermore, these tools will have to account for the features of higher and higher-level programming languages (e.g. 4th generation languages), which abstract away from machine details – from a security point of view there have to be a number of special tests on the compiled code.

There will also be tools that provide justifiable evidence that software is secure; this will mean better software assurance.

Businesses Will Have Tools To Understand and Manage Risk

We expect that risk assessment practices will be vastly better in the future, with a host of decision support tools available and a significant degree of automation. It is likely there will be standard and universally adopted security practices across enterprises, including inter-organisational and cross-layer measures, and particularly well-developed SIEM (Security Information and Event Management) systems.

Security Concerns Will Not Be A Barrier To New High Value Applications

As security practices improve and become more widely adopted, it will be easier to design high added-value applications which can make use of private and confidential information. Rather than security being seen as a barrier, we will be in a position to trust providers more and more and assume that certain fundamental security and privacy expectations will be met as a matter of common practice.

We envisage highly personalised applications and services in the areas of energy use (e.g. smart metering), assisted living, and transportation, all of which rely on the availability of highly secure technical infrastructure. Smart metering will be universally adopted, helping individuals and businesses reduce their energy costs and prevent harm to the environment. Also there will be mechanisms in place to protect critical infrastructure from failure or attack.

Another novel example of a high added-value service that will be enabled if secure systems are commonplace is vehicle-to-vehicle communication; cars will be able to authenticate and exchange location and route information, maybe interacting in ways invisible to the driver in such a way that accidents can be prevented.

3.3. A Vision for Society and the Wider Economy

Users And Businesses Will Be Accountable Online

It is only to be expected that digital crime will increase, and to account for this the Future Internet will have built-in forensics and tracking capabilities. Particularly in areas of critical infrastructure it will be possible to trace potential threat actors and install adequate protections on an ad-hoc basis. So there will be suitable audit, detection and prevention mechanisms for digital crime in the Future Internet. Also individual users will be empowered to police the network, likely reducing the need for dedicated officers. Some of the policing will likely be automated, although there will always be a need for human intervention in certain cases where legitimate behaviour is misconstrued by such systems.

There Will Be Changes In Society, Policy and Law to Cater for New Technologies

Clearly there will be fundamental changes in our perception and expectations of government; already there is a trend towards open access to government data, and we can expect 'real open government' enabled by the Future Internet. Online voting is likely to become the de facto mode of electing politicians, and politicians will need to have clear ideas and policies on citizens' digital freedoms. One might go as far as to claim that there will be notions of digital ethics, digital dignity and even digital sovereignty, all of which will be fundamental to the way citizens conduct their lives in modern society.

As mentioned before, law enforcement (policing) will change in fundamental ways, as non-compliance with the law will be automatically flagged and easily prevented; we even envis-

age the introduction of *digital sanctions* for digital misdemeanours which are enforceable, punitive, and cheaper than prison.

4. What are the Difficult Issues to Address in the Trust and Security Space?

4.1. Enabling and Empowering Individual Users

Enabling Users to Better Understand and Control Security

The first important challenge is helping users to stay safe online; this means making online security and privacy much more user-friendly; there will have to be a number of helpful defaults, namely options that are universally or widely agreed upon, so that users can avoid the arduous task of making detailed choices and carry on with their day-to-day use of the Internet. Finding the right balance between security and usability is a core challenge, and we are all too aware that there is no perfect solution.

Developing intuitive security settings or configuration options will require much research, particularly given that Future Internet systems will have to be equally usable by ICT illiterates as well as specialists. Security contexts will have to be represented in an understandable way, enabling situational awareness for users. But the most obvious challenge here is designing security into systems in such a way that it is almost invisible – thus reducing the cognitive effort required of the user; today's ICT users are already experiencing cognitive overload from the number of passwords they need to remember for different websites and applications.

Clearly there is no widely accepted notion of online trust, and more research is required in developing trust anchors for users. This is a fundamental challenge for the Internet of the future, which requires reliable indicators of trust for business and government to be conducted safely online.

In order to raise more awareness of security and the potential threats that lurk in the online world, it will be necessary to continually educate users. Users will need to be aware of their options, of the dangers and consequences of not protecting one's privacy, of the tools and technologies that exist to protect one's digital assets.

Handling Digital Identities

There already is a proliferation of digital identities in today's Internet, as individuals experiment with different personas, or more often are forced to create separate identities with different websites and providers of online services. From a privacy point of view, it may well be desirable to keep certain identities separate; in practice there will be a number of situations in which the use of a single online identity is convenient and beneficial.

How is identity management to be achieved on the multitude of devices that people use on a day-to-day basis? How will digital identities by linked to individual people? In fact, should they be? For users of services in the cloud, how will trust be conveyed between service pro-

viders? All these questions are fundamental to the challenge of developing suitable identity management for the Future Internet.

There is the challenge of developing suitable biometrics for linking physical and digital identities. Biometrics are the most obvious way of extracting information from one's physical identity, but to what extent will biometrics become socially acceptable?

Of course, in order to combat digital vandals and cybercrime it will have to be easier to identify them; maybe a tagging mechanism or a set of special flags on their digital identities. This is clearly a fruitful area for further investigation.

Dealing With Privacy Issues

There is a clear need for individuals to be able to eliminate data about their person online. There may be personal data that has been made accessible as a result of a breach, data that the individual has posted himself through error of judgement, or information that is plainly false and needs to be corrected or removed. In other words, there is a need for ways to implement the 'right to be forgotten' in the online world. It could be that systems automatically 'forget' data after a given expiry date, or that there are mechanisms in place that enable individuals to explicitly 'delete' personal data. Issues such as these have been investigated within the UK-based research project EnCoRe[7].

Another challenge relates to forensic capability and particularly the issue of traceability. It is important to be able to trace the source of a privacy breach; for this reason there is much scope for research in accountability, auditability and the corresponding tradeoffs with privacy.

Scenarios in the Future Internet that pose particular privacy concern include cloud applications and service infrastructures, as well as systems of sensor networks, namely, the so-called Internet of Things (IoT).

4.2. Developing Security Technologies for Businesses

Helping Businesses To Assess And Make Decisions About Risk Using Models For Prediction / Anticipation

What are suitable models of risk for the Future Internet? How can one accurately express security and privacy risks in complex ICT infrastructures including clouds, multiple devices, and sensor networks? These are difficult challenges, particularly as they apply across the many layers of the Internet; there is a huge amount of cross-domain security information that needs to be processed in order to adequately model risk. There will be a need for work on ever more detailed risk assessment methodologies, including particularly quantitative techniques and evidence-based risk assessment.

Business processes need to modelled in such a way that potential sources of conflict can be identified at an early stage; there are here the challenges of predicting security problems,

[7] See http://www.encore-project.info for more information.

anticipating the potential impact of certain business decisions, and figuring out where the bulk of investment in security mechanisms needs to be made. Models should be created that help managers understand ROI on security.

Security models for Future Internet need to account for different types of attackers, and there is clearly a lack of suitable meta-models for security in the different OSI layers. Furthermore, it is important to better understand the motives and psychologies of different types of attackers.

Helping Developers Build, Measure and Test Secure Systems

In order to enable businesses to provide a service without harming their interests, contracts, and general assets, there will need to be reliable and consistent methods for security testing and assurance. Not only will security need to be integrated in software development, but there will need to be adequate frameworks for certification, testing and audit.

One of the greatest promises of the Future Internet is the idea that individuals and businesses will be able to compose many different services at whim to achieve a particular goal. But how can service composition be done in a secure fashion? Is it possible to develop automatic risk reduction techniques for this? Unless the security properties of different services are formally and unambiguously specified and understood, it is certainly difficult to reason about the properties of their composition.

Testing of software of services needs to be done in an interdisciplinary fashion, so that different environments, usage scenarios and behaviours are considered. From a technical point of view, it will be desirable to have real-time testing methods and to use the computational power of the cloud to run simulations.

Building Systems That Are Resilient Against Failures and Attacks

In order to build systems that are resilient, we need to be able to model and simulate about the different types of failures and attacks that could occur. There is the challenge of making and *maintaining* models of complete systems with tools that take into account the couplings between different components. Models are just as essential for a holistic understanding of systems as for preventing low-level bugs in system code – and clearly handling and preventing software bugs is a central challenge for the future, not only in the context of Future Internet.

We expect that future software and services will need to 'evolve' and adapt to circumstances and threat environments. Real-time security is only possible if security mechanisms are designed to handle unexpected events; adaptation requires self-modifying code, which is a challenge in itself (self-protection and self-healing systems are relevant here). Also mitigation will have to keep up with the growth in system complexity.

In order to ensure overall system resilience it will be necessary to secure all the different network layers and cross-layer communications. There will have to be cross-layer trust and

accountability support; there will have to be a significant degree of fault tolerance; there will have to intrusion and vandal tolerance in applications, services, infrastructure, communities.

We do not underestimate the additional challenge of finding the right level of transparency between network level events and business activities.

Expressing And Enforcing Security Policies

There has been a significant amount of work done on the development of policy models and languages; however what is required now is a *meta-model* that encompasses features of all of these and enables interoperability between different policy enforcement mechanisms. Security policies need to be made understandable to end users, and this implies a need for visual representations and natural-language descriptions of policy rules. Due to the sheer complexity of the Future Internet, and the huge number of devices that will be interconnected, each with its own policies and data flows, there will be a need to resolve policy conflicts automatically and intelligently, rather than requiring the need for human intervention at runtime.

Enforcement mechanisms will need to be developed which ensure that client policies are adhered to on the server side. As for enforcing the law online and preventing cybercrime, there is likely to be a need for some notion of 'digital sanctions.' Because of the predicted widespread adoption of cloud computing, it is likely that control and enforcement will be required across domains and service boundaries, which is clearly a complex challenge.

Finally, we note here the imperative of achieving interoperability between policies and enforcement mechanisms from different sources, and the need to make them work well with platforms for user identification and accountability.

4.3. Broader Challenges

On the socio-economic front, there are a number of issues that will shape the world of the Future Internet:

- There will be a multitude of stakeholders, and many different ways to interact with different languages and kinds of expertise;
- There will be challenges in finding suitable business models and means of charging for Future Internet services;
- There will be an absolute need for businesses to take a holistic approach when developing FI products and services, integrating legal, societal, user, and business perspectives with technology.
- There will be a deluge of data, and a deluge of devices for accessing data (see also section 2.1.3); how this will affect the way we operate as a society remains to be seen, but it will surely impact our social interactions, the speed with which business is conducted, and the cognitive load we experience on a daily basis. Whether we can trust the data we receive and the devices we use is a challenge of central importance.

5. Approaches And Potential Solutions For Trust And Security In The Future Internet

In this section we consider some approaches that may be of use in tackling tomorrow's FI challenges, grouped here in a similar manner to previous sections: first we consider ways of empowering individual FI users; then we turn to ideas for enabling business and wrap up with broader recommendations.

5.1. Empowering Users

What can be done to give users more control of their digital lives? This is a fundamental issue from the trust and security perspective.

Development Of Universally Acceptable Digital Identifiers

We have seen that individuals' physical and digital lives are increasingly connected (section 2.1.2), that they are controlling more and more devices and desirous of the ability to customize their digital experience (sections 2.1.3 and 2.1.4). Meeting the challenges of providing usable digital identities (section 4.1.2) while providing an adequate degree of privacy (section 4.1.3) will necessarily require much interdisciplinary work; we believe that there is much to be done on the development of acceptable digital identifiers.

To address some of the above issues, there should be work on:

- an acceptable legal definition of a digital ID
- new schemas for digital identity

Education Of Citizens

As we saw in section 3.1.2, we have a vision of users being properly educated about online security and privacy risks. Clearly, in order to make the Future Internet safe, the trust and security community will need to work hard to raise awareness of security and privacy risks.

5.2. Enabling Business

There are a number of tools and techniques that could be used effectively to enable businesses to thrive in the age of the Future Internet.

Better Languages And Tools For Specifying Secure Software

This set of solutions/approaches is related to the challenges described in sections 4.2.1 and 4.2.2.

There needs to be work on developing languages and formalisms for expressing unambiguously:

- security contexts
- privacy, security and trust requirements

Tool support for reasoning and understanding contexts and requirements is essential and in particular we expect the following will be important:

- Security analysis tools integrated in software/service development environments
- Visual/graphical representation of security state for awareness and analysis
- Tools to investigate emergent properties (security, safety) of systems
- Tool support for secure system building - from the very beginning

Other related aspects that should be considered include the following:

- Model-based analysis and design and coding techniques
- Quantitative security analysis – defining suitable numerical metrics for comparing security aspects of systems and models easily
- Security- and privacy-aware service composition engines
- Better user interfaces that capture the heterogeneity of communications and elements
- Scalable security situation assessment

Improved Assurance Methods

Research and development of better assurance methods, which links to the challenges discussed in section 4.2.2 should include consideration of the following:

- Security certification for services and systems
- Development of better notification mechanisms
- Security metrics based on ISO metrology standards
- Adaptive configuration of policies and countermeasures

Privacy-Aware Software Development

As we have seen in section 4.1.3, it is fundamental for privacy to be maintained in Future Internet systems, and there should be ways for developers of FI products and services to take privacy considerations into account and enforce appropriate policies where necessary. Indeed, privacy concerns should be integrated into software development (see also section 4.2.2). Some of the technical aspects of privacy that should be addressed in the future include:

- Incorporating privacy-preserving identity management and provisioning systems into the very fabric of FI
- Deploying machine readable privacy policies everywhere
- Developing means of privacy-respecting advertising
- Developing privacy enhancing tools for social networks

- Achieving permanent deletion of digital trails with guarantees
- Developing privacy homomorphisms and cryptographic algorithms for enterprise computing, especially for cloud computing.

Development Of Rich And Expressive Security Models

We believe that there needs to be more work on the development of rich security models, which take into account the relevant legal and regulatory frameworks. Models of accountability are also very important here.

Development Of Tools For Tracking Data

We have seen that (section 3.3.1) it will be essential for Future Internet to have forensic capability, so that criminals can be identified and thwarted, and so that accountability in general can be achieved. Some of the proposed ideas that could help here include:

- Making data 'know' its origin and who's allowed to see it
- Having ontologies that describe and link data throughout the internet

5.3. Broader Recommendations

The recommendations in this session relate to the challenges described in section 4.3.

Cooperation On Issues Of National Security

International collaboration on security matters will be essential, particularly as cybercrime transcends national barriers. There should be:

- a secure and trustworthy international data exchange system for tracking cyberthreats and cybercrimes
- international standardisation of security features

Enhancement Of Legislation To Accommodate Technological Developments

An important area of work is the adaptation of existing legislation to provide adequate security and privacy protections given developments in FI technology. There should be:

- A technology aware legal framework
- A legally accepted means of offering end users a single point of trust and responsibility
- Ways of supporting law enforcement digitally
- "Digital jails": ways of temporarily penalising digital vandals

Research And Investment In Security Tools And Technology

We believe that research in the following security technologies, particularly cryptographic approaches, is very important for FI:

- Better use and novel use of cryptographic algorithms throughout the software development lifecycle
- Usable ID and trust management everywhere
- Zero knowledge leakage paradigm
- Bio-inspired protection mechanisms
- Real-time and dynamic change detection
- Strong cryptography and lightweight data mining that can be executed on nanoscale devices
- Developing cryptography for use in the cloud

Consideration Of Novel, Radical Approaches

The following are germs of ideas that are subject to further development, and we will not expand on the details in the current version of this document.

- Automatic periodic security and trust re-evaluation and certification
- Disposable systems (think virtual!)
- Loosely coupled systems
- Code will be reused more and more
- Intrusion tolerance for services, workflows, communities
- Resilient, Trust-enabling architectures, e;g trusted collection of security data from heterogeneous networked devices (IoT)
- Inter-disciplinary groups work effectively together

6.List of Contributing Research Projects

The material presented in this report has been collected, researched and summarised by Nick Wainwright and Nick Papanikolaou (HP Labs) of the EFFECTSPLUS project. The content was gathered from workshop participants; the full list of research projects that participated in these workshops is below.

- ABC4TRUST - https://abc4trust.eu/
- ANIKETOS – http://www.aniketos.eu/
- ASSERT4SOA – http://www.assert4soa.eu/
- BIC-TRUST – http://www.bic-trust.eu/
- CASAGRAS2 - www.iot-casagras.org/
- COMIFIN - www.comifin.eu/
- DEMONS - www.fp7-demons.eu/
- ECRYPT - www.ecrypt.eu.org/
- EFFECTSPLUS – www.effectsplus.eu
- ELLIOT - www.elliot-project.eu/
- ENDORSE – www.ict-endorse.eu
- GINI-SA - www.gini-sa.eu/
- MASSIF - www.massif-project.eu/
- MOSIPS - www.mosips.eu/
- NESSOS - www.nessos-project.eu/
- PASSIVE – ict-passive.eu/
- PICOS - www.picos-project.eu/
- POSECCO - www.posecco.eu/
- PRIMELIFE – primelife.ercim.eu/
- SECURECHANGE - www.securechange.eu/
- SEPIA – sepia-project.eu/
- SERSCIS - www.serscis.eu/
- SESERV - www.seserv.org/
- SYSSEC - www.syssec-project.eu/
- TAS3 – vds1628.sivit.org/tas3/
- TCLOUDS - https://www.tclouds-project.eu/
- TWISNET - www.twisnet.eu/
- UTRUSTIT - www.utrustit.eu/
- VIKING - www.vikingproject.eu/
- WEBINOS – webinos.org/
- WSAN4CIP - www.wsan4cip.eu/