UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- inforewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP

Cover page designed by Concha Arias-Pérez
"DNA in love" / © CEPIS 2010
Layout Design: François Louis Nicolet
Composition: Jorge Llácer-Gil de Ramales

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (August 2010)

"2010: Emerging Information Technologies (II)"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. XI, issue No. 3, June 2010

Monograph: 2010 - Emerging Information Technologies (I)

(published jointly with Novática*)

Guest Editors: *Alonso Álvarez-García, Heinz Brüggemann, Víctor-Amadeo Bañuls-Silvera, and Gregorio Martín-Quetglas*

UPENET (UPGRADE European NETwork)

CEPIS NEWS

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Security 2.0: Facing up to the Tsunami

Enrique Díaz-Fernández, Miguel Ochoa-Fuentes, David Prieto-Marqués, Francisco Romero-Bueno, and Vicente Segura-Gualde

We live in times of constant technological progress in which new paradigms and technologies, such as the "Internet of Things", "Semantic Web" or "Cloud Computing" are constantly appearing and promising to make our lives easier. However, the same security problems as always (theft of personal data, denial of service attacks, industrial espionage…) continue to concern us, even more so due to our growing dependence on information technologies. Faced with such a shifting scenario, we need to adopt a strategy with a global approach to confront the ever-present security threats. We believe that this approach should be based on three axes: a) security of infrastructures; b) security based on collaboration between parties; c) security of the individuals, focusing on digital identity and ensuring its privacy. In this article we describe our vision of how we can withstand the tsunami of security problems.

Keywords: Identity, Monitoring, Privacy, Reputation, Security.

1 Introduction

Nobody today can be unaware that our growing depend-

Authors

Enrique Díaz-Fernández graduated as a Telecommunications Engineer from the *Universidad Politécnica de Madrid*, Spain. He has pursued his professional career in Telefónica Investigación and Desarrollo, a Spanish company which he joined in 1997, after having worked there as an intern since 1995. Practically from the outset his work has been related to the field of security of Telefónica's various IP networks. Since 2006 he has been Divisional Head in the Security and Trust in Networks and Services department and he is currently the coordinator of the project Segur@, a project subsidized by the CDTI as part of the CENIT programme, in turn part of the Ingenio2010 initiative, which is researching into new technologies in the field of ICT security and trust. <ediaz@tid.es>.

Miguel Ochoa-Fuentes graduated as an Informatics Engineer from the *Universidad Politécnica de Madrid,* Spain. He started his collaboration with Telefónica I+D in 1998, performing consultancy work in end-user application projects. He became a full-time member of staff at Telefónica I+D in 2001, where he has pursued his career in the field of logical security in projects such as "ATICO", eFactura de Telefónica de España, etc. His work during these years has centred on the technology of public key infrastructure, smart cards, and digital identity management systems. He has participated in the implementation project for an electronic certification infrastructure for Canal de Isabel II, among other projects. His work is currently focused on identity and privacy management activities in the Cenit Segur@ project. <ochoa@tid.es>.

David Prieto-Marqués graduated as a Telecommunications Engineer from the *Universidad Politécnica de Madrid*, Spain. He has pursued his professional career in Telefónica Investigación and Desarrollo, a Spanish company which he joined in 2000, after having worked there as an intern since 1998. Initially his work was related to communications technologies and access to Telefónica's various IP networks, both in Spain and in various Latin American countries. In 2002, as Project Manager, he collaborated in the roll-out of audiovisual and multimedia service platforms over ADSL (Imagenio, Mundos ADSL, etc.) for Telefónica de España. Later, now in the field of security, he collaborated in consultancy projects for service-oriented architectures, and since 2007 in innovation activities in the field of the technologies of identification, authentication and network access control through the Cenit Segur@ project. <dprieto@tid.es>.

Francisco Romero-Bueno graduated as an Informatics Engineer from the *Universidad Politécnica de Madrid,* Spain. In 2001 he joined the Euro6IX project as an intern developing a prototype intrusion detector for IPv6 networks. When his grant ended he continued to collaborate in other European projects, such as EuQoS and Ambient Networks, in which his work was oriented towards the monitoring of traffic from a content provision point of view. In 2007 he became a full-time member of staff at Telefónica I+D where he returned to security-oriented network monitoring through the Cenit Segur@ project, where he is currently evaluating new technologies for the detection of malware, such as the construction of traffic models and anomaly detection, or event correlation, and he designs and develops prototypes based on those technologies. <frb@tid.es>.

Vicente Segura-Gualde graduated as a Telecommunications Engineer from the *Universidad Politécnica de Valencia*, Spain, and obtained his CISSP Certificate (Certified Information Systems Security Professional). In 2001 he joined Telefónica I+D as an intern to work on the EURESCOM project studying the interoperability of public key infrastructures. In 2002 he became a full-time member of staff at Telefónica I+D and since then he has collaborated in various security projects for different Telefónica Group business units, including projects devoted to information system security, the design and roll-out of architectures for the secure publication of web services, and engineering activities in security supervision systems, among other fields. His work is currently focused on the field of innovation in security risk analysis in the Cenit Segur@ project. <vsg@tid.es>.

ence on information and communication technologies makes us increasingly more vulnerable to any security problems that may arise. These security problems evolve constantly in pace with technological developments and often at an even faster pace.

Meanwhile, unlike other information and communication technologies, security and privacy are cross-sectional issues. It could be said that they are a sort of fluid which must surround not only the spaces that the other technologies leave between them, but also the spaces left inside each technology. Security and the privacy do not constitute the essential purpose for which any technology was created, but they are nevertheless essential properties of that technology. And they are properties which, if absent, will penalize the technology, although its presence is not normally valued as highly as it should be.

These two characteristics, quickness to change and cross-sectionality, must be taken into account when addressing security problems. But before revealing our vision of how to address these problems, first we need to examine the security issues facing our society today.

People often speak of security and privacy problems in a broad sense to refer to all concerns related to these matters. Thus botnets or malware are security problems, as are phishing or pharming, cyberbullying, poor usability of security, or child protection solutions. However, clearly not all these problems are of the same kind, nor can they be addressed in the same way. For example, the poor usability of security solutions is a design problem consisting of the incapacity of software to tailor its messages to the context and to the user's level of knowledge, so the man-machine interface is not effective in these cases. However, botnets represent a problem of another kind. On the one hand, it is easy and cheap to create them, thanks to the large number of PCs accessible by Internet without any proper protection measures, and as a result of their owners' ignorance and/or lack of interest in strengthening the security of their machines. On the other hand, there are many ways of obtaining a monetary benefit from botnets: spam, DDoS attacks, theft of personal data…

Therefore, the first step in developing a security strategy is to identify and characterize these problems. We have identified three types of security problems, which we describe below:

- Threats: the events which by themselves cause harm. In a broad sense, these events may be either criminal acts caused intentionally or involuntary acts (errors), natural catastrophes, or fortuitous accidents. This article focuses mainly on the former. Examples of these types of problems are spam, phishing, denial of service attacks, and theft of confidential information.
- Tools: these are the instruments used by attackers to cause the harm. By themselves they are not threat, but they are the tool used by the attacker to commit the criminal act. Unlike threats, the tools themselves do not cause any harm. It might be said that they are the weapon which the attacker uses to commit the crime. Examples of such tools are: botnets, malware, and social engineering techniques.
- Facilitating factors: this refers to factors of various kinds (social, economic, political, the design of security technologies) which help generate a climate which hinders the generalized development and use of security technologies and/or facilitate the proliferation of threats or tools. Some examples of these are:
- Limited sharing of security data among organizations. Today the level of cooperation between organizations is not sufficiently well developed to react rapidly and effectively to the appearance of new threats.
- Poor usability of security solutions. Experts agree that existing security solutions are not designed to be used by users with only a basic knowledge of computing, which partly explains the large number of machines which fail to meet the minimum security requirements to connect safely to the Internet [1].

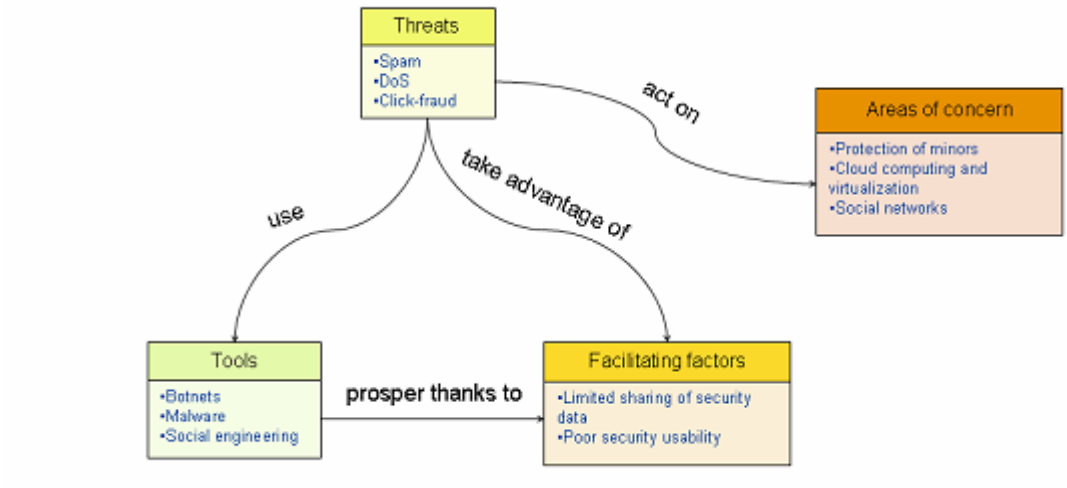

Figure 1: Categories of Security Problems and how they relate to One Another.

Alongside these categories of problems we can also identify three areas of concern; i.e., areas in which security problems are especially important due to the interest they arouse at any moment for some reason (the alleged technological revolution, due to some legal obligation, due to their impact on society…). The speed with which areas of concern change requires the teams responsible for security to be flexible and have a great capacity to acquire the knowledge they need to keep up with developments in these new areas. Examples of areas of growing concern: child protection, social networks and virtualization, and cloud computing technologies.

Figure 1 outlines the relationships between the different categories of security problems described above and lists a few representative examples of each one.

On the one hand, threats make use of the tools available to automate certain tasks. Thus, for example, for spam or distributed denial of service attacks to prosper, botnets are used to send mass emails and to saturate resources respectively, while fraud based on simulating clicks on web links to obtain advertising revenue (click-fraud) uses specially designed malware.

On the other hand, threats and tools take advantage of the environment created by facilitating factors to prosper. Thus, factors such as the poor usability of security tools or the lack of interest on the part of the owners of machines to solve security problems, facilitate the creation of large bot networks. Also, the limited sharing of data among organizations hinders the development of effective methods of coordinated response.

It should also be noted that threats can act on different areas. Each of those areas will have its own characteristics and need to be taken into account when analysing a threat in that context.

2 Lines of Action

In order to address the above security problems, we have identified three lines of action covering the three types of problems (threats, tools and facilitating factors) facing the different areas of concern.

The threats and tools cannot be combated solely from the perspective of the Internet user or the infrastructure itself. We need to put a strategy into place which combines user-centred solutions with network-based solutions.

For this reason, two of the three lines of action are infrastructure security and the protection and privacy of individuals.

The third line of action focuses on the facilitating factors. In this field we turn to solutions based on cooperative security management. These solutions depend on the development of security information exchange schemes that enable us to discover and react as quickly as possible to new threats as they appear.

Naturally, for all these lines of action, the usability of the solutions is an essential aspect, one which we consider to be a key success factor, especially if the solution is intended for the general public.

2.1 Infrastructure Security

Many of the above mentioned security problems in areas of recent concern are propagated through unusual channels or media, such as social networks. This makes it practically impossible to prevent them by using traditional solutions, which leads us to think that the security of the infrastructure should be improved, on the one hand, by strengthening its structure and, on the other hand, by providing it with more intelligence to enable it to offer security in the application layer. Network security can also be provided as a service for other applications through standard frameworks such as IMS (IP Multimedia Subsystem) or SDP (Service Delivery Platform).

We consider that this line of action should focus on developing that network intelligence in order to assess the reputation of traffic sources and take action against them if they look as if they might cause problems or undesired behaviours.

According to the C.U.P. dictionary, reputation is defined as "*the opinion that people in general have about someone or something, or how much respect or admiration someone or something receives*". Therefore, from the point of view of the network, in order to form an opinion about any source of traffic, the most information as possible about that source needs to be gathered and analysed in real time. This information will originate, on the one hand, from the behaviour that it displays in the network (as we explain in the next section) and, on the other hand, by being capable of assessing the status of that source at the access to our network. Once this information gathering has been completed, we need to analyse all the information on the basis of a set of pre-defined criteria (also called policies), in order to form an opinion which will determine the actions which are to be permitted to the traffic source within our network. It is essential that the analysis of that information and, therefore, of the source's reputation is performed in real time, so that the network can react if any undesired event should occur.

The gathering of this information in a reliable manner is a major challenge, since we should not forget that the opinion formed by the network will have the same degree of integrity as its information sources. Information can be gathered either from the network, which will mean achieving a limited degree of detail but with a high level of reliability, or using agents or facilitators of that information to be found at the source of the data itself. Obviously, in the latter case, the network will have much more detailed information but its reliability will depend on the facilitator's integrity. As we can see, the two approaches have their limitations when used separately, so it is vital to combine the two strategies.

Another challenge currently presented by these technologies is mobility, possibly an even more important issue if we bear in mind the increase in the number of mobiles with Internet access and the growing number of people who work or do business remotely. For this type of cases, we need to progress in terms of standardization when examining the status of any data source, and in terms of interoperability between the various network nodes to communicate the

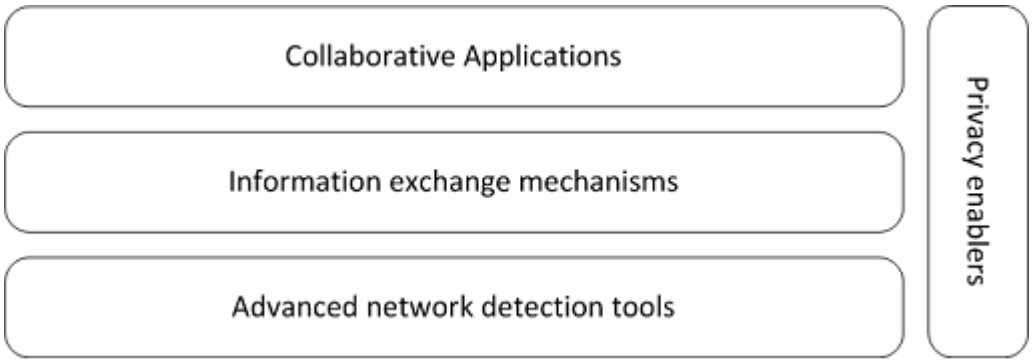

Figure 2: Challenges of Collaborative Security.

policies and be able to share "*opinions*" abut sources. We should not forget that, as happens with people, at the end of the day the opinion or trust we have in a network element often depends on what is observed, but also depends on what nearby elements can tell us.

Therefore, bearing in mind all these challenges, when it comes to reputing a data source, we believe that solutions should not be limited to appraising aspects such as the user of that source or whether the source has certain software running, but rather solutions should consider all the possible components the network operator may have. Prototypes are currently being developed to enable not only the dimensions of the traditional solutions to be included but also others, such as location of the source, the authentication of its hardware, or strong authentication mechanisms such as vascular or fingerprint-based biometrics.

Also, in order to take these trust or reputation technologies to all possible environments from where a user can connect to the network, trust scenarios are being implemented in the mobile communications and home environments, in the latter case making it possible to assess the security of devices such as IP phones.

Another major challenge will be how and where the network will perform the actions appropriate to the idea or opinion that has been formed in respect of any element wishing to interact with it. Here we need to consider a much wider range of possibilities, since depending on the point at which the actions (enforcement) take place, they could be more specific or more general. For example, distributed measures could be applied at the endpoints, at the network devices closest to the data source or to the entry point of that data source to our network. Obviously, if the measures can be applied at the endpoint itself, they could be tailored to the needs of each user, by acting on the applications on the user's machine, but if measures are taken on elements belonging to the network, they will have to be grouped together, being actions of a more general nature. With this idea in mind, and considering aspects such as mobility, various approaches are used to address this issue. On the one hand there are those who try to apply the measures in a decentralized manner – an example of this could be a distributed firewall [2] - , and on the other hand, there are those who try to base their solutions on device virtualization [3] and on in-the-cloud security services.

2.2 Collaborative Security Management

"*The threats of today require solutions of today*." That sentence is worthy of being carved in stone. Or is anyone thinking of fighting against botnets, say, not by monitoring their machine but their domain? In this case, what percentage of infected machines could an operator like Telefónica eradicate by itself? The truth is that we do not even know for sure just how widespread these malware tools are, so any kind of estimate would always be just that, an approximation to the solution of the problem, but not the solution per se. The fact is that cases like this, and others such as distributed denial of service attacks, spam generated in remote domains with a local impact, and the worldwide propagation of viruses in a matter of hours, can only be addressed through a global approach involving the various network management entities, by exchanging information, collating their results, setting up policies that go beyond local interests..., in short, by collaborating.

However, we believe that collaboration at this level involves at least four challenges (see Figure 2). Meeting those challenges must be the focus of all monitoring-oriented innovation in the coming years.

The most immediate challenge is to define the cooperative applications themselves. These applications need to have forward intelligence for the purpose of detection, correlation and response, and must boast a high level of automation in terms of self-configuration, adaptability and proactivity. Examples of this approach can be seen in proposals aimed at the global detection of botnets by gathering inter-dominion information. There is also a trend towards the use of expert event correlators to process low level events into more compact and therefore more usable events. These will have developed from the traditional event correlators of commercial SIEMs, which are based on a large number of static and inflexible rules, while the use of expert systems provides a high level of adaptability to new threats with a significant reduction of correlation meta information. Another type of state-of-the-art development is the dynamic risk analysis of security events as they hap-

pen, which, at a more strategic than operational level, will identify the risk to which assets are exposed. As can be seen, the possibilities in this field are practically boundless and all in-the-cloud security tools, for example, also seem to lean towards this approach.

The following challenge that we will be mentioning here is that of setting up information exchange mechanisms. By which is meant information exchange in any of its manifestations: publication, dissemination, subscription, etc. Here there is a significant use of peer-to-peer networks, whose appropriateness for such a purpose has been proven over recent years. But it is not only a matter of defining the protocol; we need to define a whole set of interfaces and facilitators which make the task of the developer of the high level applications we have seen previously so much easier.

No less important than the sharing of data is the anonymization of that data in order to ensure the privacy of users, a right which users enjoy regardless of the security management entity, which we see may be very remote.

Finally, the collaborative security at this level would make no sense without a strong commitment to network monitoring tools. And, since the devices of the future will always be connected, will be mobile and, most importantly, will be of every kind imaginable, the monitoring services appropriate to each one will only be able to be provided over the network. This strategy also provides for a dissociation between the end user who benefits from the security and the tools which provide it, which will avoid what tends to be one of the weaknesses of any security scheme. As we have said, the tendency is to monitor from the network, by making use of either well-known but limited paradigms, such as pattern detection, or advanced paradigms, such as behaviour modelling and anomaly detection. By modelling the behaviour of both users and systems and services, we can establish a base line from which it is possible to identify deviations in network use, times or traffic characteristics, among others, which is very useful, not only for detecting current threats but future ones too. And all this based on the new general purpose hardware which is emerging precisely for the implementation of these solutions (and others) directly in appliances or routers, which will enable them to work at line speed, given their total integration with the network nodes.

2.3 Identity and Privacy

Starting from the initial problem that the Internet was built without any way of knowing who was going to connect to what, the massive use of the Internet for every kind of electronic transaction require companies and public and private organizations to have an identity layer on top of the Internet which enables them to identify their interlocutors.

The concept of digital identity management (IdM) can be defined as the management of the lifecycle of the personal information necessary to identify an individual when he or she accesses products or services on line. From the viewpoint of organizations, they not only need to ensure that the person accessing the service is the right person, but they also need a rapid, flexible and standardized manner of aggregating all the information for the same user.

But private individuals may view with suspicion the uncontrolled collection of their attributes that make them identifiable and traceable in the digital world. Last year one of the biggest US employment websites published a study which revealed that half the employers interviewed used social networks to filter possible candidates [4]. This trail of information is a digital shadow which will follow them in every interaction with the network and it will be very difficult, not to say impossible, to erase. For this reason, if an identity management solution is to be successful, it must be designed in such a way as to respect the privacy of individuals. Privacy by design [5] is a new approach in which conformity with privacy and the data protection must be designed from the outset in systems that store personal information, instead of patching privacy holes as they appear or simply ignoring them. Among the principles behind this practice are prevention, privacy by default, end-to-end protection, visibility and transparency, which enables individuals to have greater control and decision over what personal data they share and with whom.

The federation of identities is a set of technologies and processes which solves the problems posed by both organizations and individuals, and enables organizations to delegate identity tasks through security domains, aggregate user information from different sources with the prior consent of that user, and provide personalized services with enhanced usability for their users, such as that provided by single sign on (SSO). SSO solutions reduce the to and fro of credentials over networks and enables identity providers to specialize in strong authentication mechanisms, protecting users from the much feared threat of identity theft. Similarly, the creation of trust relationships between federated web services is an efficient defence against phishing. Although, paradoxically, these costly relationships are the ones that are causing initiatives to emerge that are lighter but less secure for the user.

Faced with this challenge, industrial consortia, standardization organizations, open-code communities, and major companies have developed a wide range of identity applications, services and protocols, creating a major confusion in the identity management market as a result of such technological dispersion. In an attempt to put an end to this diversity of solutions to the same problems, the Kantara initiative [6] has recently emerged as a review of the Liberty Alliance strategy with the idea of creating common collaborative space in which to guide the evolution of identity management. Thus initiatives such as Liberty Alliance, Concordia, DataPortability, and the Information Card Foundation have brought their different approaches to the same space in an attempt to address the new challenges posed by identity management.

The three identity management initiatives currently considered to be the most popular, although due to their different approaches they are not mutually compatible, are: SAMLv2 [7], OpenID [8] and Windows CardSpace [9]. This

incompatibility becomes apparent when a user authenticates to a system using a specific identity management architecture and cannot use a service provider which uses a different architecture, since this would require the user to authenticate again.

In the absence of a unified technology, our approach consists of seeking interoperability between these solutions by offering integration which is transparent to users, and providing them with the possibility of using different identity management systems without having to worry about compatibility.

The role of identity in service development platforms can be approached in one of two ways.

On the one hand, from a more traditional perspective of security, we need tools aimed at allowing users to control the sharing of their personal information and access to services by third parties who could act in their name. The sharing of personal information is a major concern regarding the administration of privacy, data protection, and compliance with the law. Delegated authorization systems are being postulated as de facto standards. OAuth 1.0a [10], a lighter version which has profiles for desktop and mobile device applications (OAuth WRAP), and their joint evolution to OAuth 2.0, are attracting the attention of what is known as the Web 2.0.

On the other hand, and here lies a new potential, identity can be seen as a specific capability provided by the network, on which to build trust generating services. Identity as a service, or IdaaS, provides a consistent and reusable identity for all applications and services which may require one. These identity services include, among other federation services, authentication, authorization, auditing, and the provision and administration of identities and roles.

3 Conclusions

In this article we have attempted to cover the many and varied reasons for the security risks affecting ICT. The problems causing those risks can be classified into three major categories: tools, threats and facilitators. On the basis of this classification we can devise a strategy based on three lines of action with which to address security risks in a global manner.

The purpose of two of these three lines of action, infrastructure security and collaborative security management, is to strengthen the infrastructure itself and make it more intelligent so that it can analyse the information in its environment, making the best decisions at any given time. Analysis requirements may be covered to a great extent by intelligent nodes containing collaborative applications, while reputation management can take care of everything to do with the decisions.

The third line of action, identity and privacy of individuals, aims to compatibilize the growing presence of users on the network with the protection of their intimacy. Identity federation helps users in their experience in the use of services. But these systems will not be successful unless personal privacy is taken into account.

References

[1] Bruce Schneier. "Security vs. Usability". Blog "Schneier on Security" <http://www.schneier.com/blog/archives/2009/08/security_vs_usa.html>.

[2] S. Ioannidis et al. "Implementing a Distributed Firewall". Proc. Computer and Communications Security (CSS), 2000; <http://www.itsec.gov.cn/webportal/download/2004_ccs-df.pdf>.

[3] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield. "Xen and the art of virtualization" B. ACM SIGOPS Operating Systems Review vol. 37:5, pp 164-177, 2003, pub. ACM New York, NY, USA.

[4] The Hiring Site. <http://thehiringsite.careerbuilder.com/2009/08/20/nearly-half-of-employers-use-social-networking-sites-to-screen-job-candidates/>.

[5] Privacy by Design. <http://www.privacybydesign.ca/>.

[6] Kantara Initiative. <http://www.kantarainitiative.org/>.

[7] OASIS. Security Services (SAML) TC, <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security>.

[8] OpenID Foundation. <http://openid.net/>.

[9] Microsoft. Microsoft Windows CardSpace, <http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx>.

[10] Oauth. Oauth Community Site, <http://oauth.net>.