15

Trust in an Asynchronous World: Can We Build More Secure Infrastructure?

Dragutin Vuković
INKUS Ltd.
Croatia

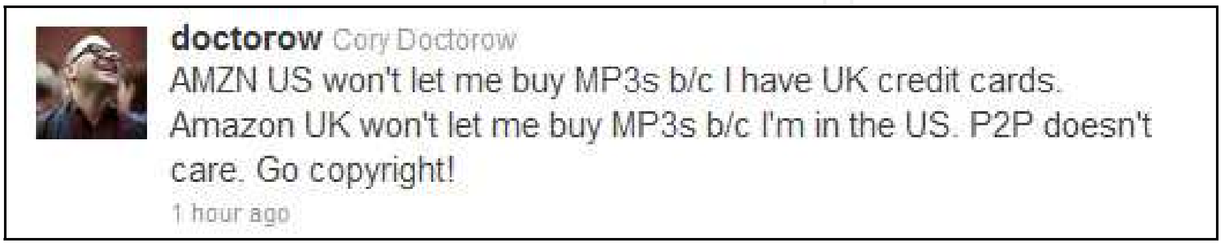
1. Introduction

Through history, many methods were designed and used for secure transfer of confidential information. During the WWII Allied Forces developed a method for securing phone conversation which included a pair of synchronized phonographs playing identical copies of white noise records. This method, called SIGSALLY, a.k.a. X System, Project X, Ciphony I or Green Hornet, used as secure speech system for the highest-level Allied voice communications (Fagen, 1978), is a very literal example of synchronicity because it would not work at all if there was no perfect synchronism maintained between phonographs at both ends of a voice channel. Other methods were devised for military communication by all participants, to mention only the famous German Enigma machine (Winkel, 2005). The common denominator of these historic methods is that all of them need a synchronicity in one way or another – synchronous keys, one-time-pads, etc. Therefore, when collaborating on matters that include a risk of information abuse, traditional approach calls for a synchronous procedure, that is, if there is a need to transfer some confidential information from one person to another, both persons will agree to meet at the same place, at agreed time. They will meet and authenticate each other by agreed procedure; third party may be involved to secure authentication. Information will be exchanged on agreed medium and participants will part assured that information is exchanged in a secure manner. This is an example of synchronous procedure, meaning that all participants have to be in contact at the same agreed time and the information is under control of a trusted party during the whole transaction. Synchronicity of the procedure is historically a prerequisite for establishing the trust relationship between participants of information exchange.

Procedures to transfer and store information in a secure manner are deployed in computing and communication networks in various forms and technologies, but they are basically all drawing on the same principle of synchronicity. With the development of Internet technologies, transfer and storage procedures are becoming more asynchronous. This means that not all parties involved are in contact at the same time, information could be, for a period of time, left into the custody of a party whose trust, and even authenticity, is not completely assured.

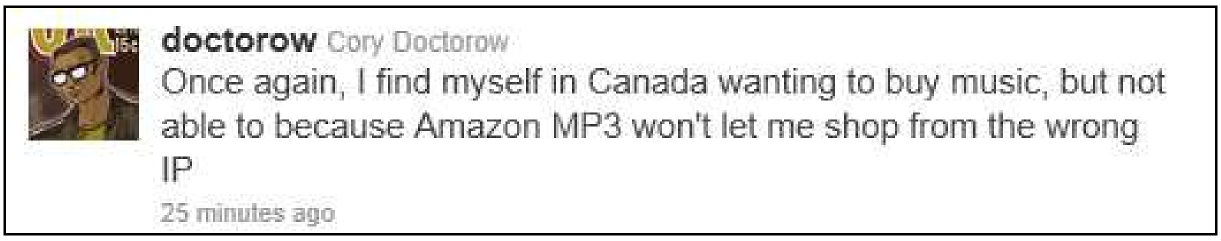
From this, we are witnessing many problems with exposed personal information such as stolen identity abuse, credit card fraud, not to mention the confidential information leakages from stolen computers and media not properly protected. Consequently, there is a diminution of customers' confidence in IT services and especially when provided through public network. Users want to be assured that their data are safe and secure with service provider. On the other side, service providers want to be assured that theirs services will be properly paid for. Some other confidence issues can be identified as well. Service providers are increasingly worried about risks their businesses are exposed in such environment, and they are building layer upon layer of information security technology to protect their customers' information as well as their shareholder value.

To illustrate this lack of confidence on the service providers' side, we will present recent 'tweets' by Cory Doctorow – famous writer, blogger and activist (see Figures 1 and 2).



doctorow Cory Doctorow
AMZN US won't let me buy MP3s b/c I have UK credit cards. Amazon UK won't let me buy MP3s b/c I'm in the US. P2P doesn't care. Go copyright!
1 hour ago

Fig. 1. Cory Doctorow's tweet on 2011-06-06T13:00



doctorow Cory Doctorow
Once again, I find myself in Canada wanting to buy music, but not able to because Amazon MP3 won't let me shop from the wrong IP
25 minutes ago

Fig. 2. Cory Doctorow's tweet on 2011-08-06T19:00

Cory Doctorow is a citizen of United Kingdom, born in Canada. During his travel to the USA, he wanted to buy some music from Amazon US, but Amazon US did not have confidence in Doctorow's UK credit cards. He then tried to buy music from Amazon UK, but Amazon UK did not have confidence in Doctorow's current location (i.e.: IP address) which happen to be in USA at the moment. Similar lack of confidence is observed again by Doctorow shortly later as he travelled to Canada.

Such lack of confidence, albeit frequent at current level of Internet technology development, is hindering further proliferation of on-line services, causing dissatisfaction of all parties involved, customers and service providers – customers because of inability to access services they are willing to consume and spend for, and providers because of potential markets being unutilised.

It is our belief that the cooperative behaviour in on-line services can be greatly improved by utilizing appropriate functions in the underlying infrastructure to foster trust and confidence between customers and on-line services providers. This belief is based on our conclusions inferred from the research in several fields spanning sociology (confidence, trust), technology (networking, communication, Internet technologies), and management (identity, information security):

- Confidence stems from trust, and trust is established between entities which are represented by their identities (Benantar, 2005), (Six, 2005).
- In computing and communications technology, the concept of trust is generally bound to reliability and dependability, which is a misconception in the sense of establishing the trust relationship between customers and on-line services regarding information security (Smith, 2005), (Serpanos, 2011).
- There are information technologies ready available and capable of supporting and enhancing trust relationship between various on-line systems but their deployment lacks systemic approach, i.e. they are utilized in specific services, thus multiplying non-trust boundaries which have to be handled on a per-case basis (Lerner *et al.*, 2002), (Mather, 2009).

These findings led us to the research question addressed in this chapter – could we envision a model for distributed computer system which would foster sociological notions of trust and confidence within the infrastructure? Model implementations would then utilize existing technologies and solutions in a systemic way to enforce establishment of stronger trust relationships between virtual digital entities, promoting confidence in on-line services regarding information security and enabling cooperation.

In this chapter we first discuss, in Section 2, the flow of information on the Internet and how it becomes more and more asynchronous with the proliferation of advanced technologies. Then we give an overview of risks involved due to asynchronous nature of data storage, transfer and processing in contemporary Internet technologies, in Section 3. Section 4 provides some insight about the notion of trust, its relation to confidence and its role in distributed computer systems. New and enhanced architecture of distributed computer systems, named *multilevel cell distributed computer system architecture*, to be utilized through the internet, is proposed in Section 5. Section 6 discusses, using trust-confidence-cooperation (TCC) model, how the cell architecture can provide enhancements to cooperation in on-line business. Some closing afterthoughts are given in Section 7.

2. Asynchronicity in modern communications

We infer from Section 1 that synchronicity is the underlying principle of security procedures in various areas, including information transfer and storage which is of main interest to us. Then, with new technologies in the IT age, synchronicity was sacrificed to achieve customer friendliness via speed, but this introduced asynchronous solutions, which is expanded on next.

Problem with synchronous procedures is that they spend time waiting for synchronization events to co-occur, adding to the overall length of the procedure. This was not the problem while the information transfer itself was comparably slow, so that overhead incurred by synchronization took only a small fraction of message duration. Shape of things has changed with the emergence of Internet. Nowadays, when high speed wired and wireless communication is omnipresent, everything is happening much quicker than before. Every part of world is accessible and digital information can be transferred with incredible speed. These speeds are made possible both by pure technological advances in electronic communication circuitry and by the fact that most data transfer technologies at physical, data link layers are asynchronous.

Our way of life changed accordingly. We learned to exchange large amount of information on a regular basis and we expect it to happen almost in real time. That is why we can send photos to our friends right from the field, and we expect their comments to come back to our smartphones in minutes. This can also be achieved despite geographical dispersion of people and varying frequency of when we meet. In order to enjoy this convenience we are ready to loosen our expectations regarding confidentiality and privacy of our information. Thus we entered asynchronous mode of operation, letting things happen more quickly, on the expense of some security issues.

On the other hand, when we come to information whose confidential nature we want to maintain during transfer and storage, we still at present stick to synchronous methods, having them proved successful before (perceived performance) and finding them acceptable among methods offered (value similarity). We will use cryptographic methods synchronized by exchanging keys, secure services bound by strong contracts, enforced by law. Or we may simply fall back to old-fashioned method of delivering information personally, possibly having it written only in messenger's memory, a communication channel with small bandwidth and large delay, having unreliable information storage.

Special category of information that we are interested in securing, are bound to transfer of financial value, such as electronic funds transfer, electronic money, credit cards, or anonymous debit cards (Androulaki, 2009), but this is a whole area on its own, which will not be discussed here although this area may also benefit from confidence and trust enhancements provided by architectural concepts discussed.

Reality is that we want more and more information to be transferred at higher and higher bandwidths, having smaller and smaller delays, with more and more confidence. The emergence of Web 2.0 applications and proliferation of cloud computing paradigm made our expectations only bigger, and asynchronicity more certain.

Cloud computing appears to have emerged very recently as a subject of substantial industrial and academic interest, though its meaning and scope, fit with respect to other paradigms is hotly debated. For some researchers, clouds are a natural evolution towards full commercialisation of grid systems, while for others they may be dismissed as a mere rebranding of the existing pay-per-use or pay-as-you-go technologies. From either perspective, it appears that 'cloud' has become the label of choice for accountable pay-per-use access to a wide variety of third-party applications and computational resources on a massive scale. Clouds are now supporting patterns of less-predictable resource use for applications, services across the IT spectrum, from online office applications to high-throughput transactional services and high-performance computations involving substantial quantities of processing cycles and storage. The current notion of clouds seems to blur the distinctions between grid services, web services, and data centres, amongst others, and brings considerations of lowering the cost for relatively bursty applications to the fore.

Cloud computing is a new way of delivering computing resources, not a new technology. Computing services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. Since we are in a time of belt-tightening, this new economic model for computing has found fertile ground and is seeing massive global investment. According to IDC's analysis, the worldwide forecast for cloud services in 2009 will be in the order of $17.4bn (IDC 2009, as cited in

Catteddu, 2009). The estimation for 2013 amounts to $44.2bn, with the European market ranging from €971m in 2008 to €6,005m in 2013 (Bradshaw 2009, as cited in Catteddu, 2009).

There is probably no other field of research with as huge amount of literature than the field of modern data communication and Internet, especially when looking in publishing rate terms (number of titles per unit of time). Therefore it would be quite unwieldy to produce a thorough overview of literature in this field. Here are some pointers to titles that could provide good starting point for interested readers to investigate further in the field:

- Data transfer and communication technologies as building substance of Internet: (Lerner *et al.*, 2002), (Governor, 2009), (Sobh *et al.*, 2010), (Sorensen, 2010), (Preve, 2011), (Serpanos and Wolf, 2011).
- Middleware and Internet: (Lerner *et al.*, 2002), (Puder *et al.*, 2006), (Toninelli *et al.*, 2011), (Georgantas *et al.*, 2011).
- Contemporary technologies and paradigms in Internet – Web 2.0, grid and pervasive computing, cloud computing: (Mattern, 2006), (Puder *et al.*, 2006), (Reese, 2009), (Governor, 2009), (Rittinghouse and Ransome, 2010), (Zheng, 2010), (Zagalo *et al.*, 2011).
- Identity and privacy in distributed systems: (Benantar, 2005), (Windley, 2005), (Waldo *et al.*, 2007), (Nin and Herranz, 2010), (Sileo, 2010), (Papacharissi, 2011).

With this in mind, we are ready to probe the risks in the asynchronous world, which is done next in Section 3.

3. Risks in an asynchronous world

According to analyst firm Gartner, cloud computing is fraught with security risks (Brodkin, 2008). Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor. Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing," Gartner says.

According to Gartner, before selecting a cloud vendor, customer should raise seven specific security issues (Brodkin, 2008):

1. **Privileged user access.** Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring, oversight of privileged administrators, and the controls over their access.
2. **Regulatory compliance.** Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signalling that customers can only use them for the most trivial functions.
3. **Data location.** When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. **Data segregation**. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. Find out what is done to segregate data at rest. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability.
5. **Recovery.** Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has the ability to do a complete restoration, and how long it will take.
6. **Investigative support.** Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located, may also be spread across an ever-changing set of hosts and data centres. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.
7. **Long-term viability.** Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. Ask potential providers how you would get your data back, if it would be in a format that you could import into a replacement application.

In the paper edited by Daniele Catteddu and Giles Hogben, (Catteddu, 2009) published by The European Network and Information Security Agency (ENISA) in the context of ENISA's Emerging and Future Risk programme, a group of selected industry, academic and government experts in the subject area, expressed their opinions about benefits, risks and recommendations for information security in cloud computing. Experts identified a number of cloud specific risks, the most important of which we will enumerate here:

1. **Loss of governance.** In using cloud infrastructures, the client necessarily cedes control to the cloud provider on a number of issues which may affect security. At the same time, service level agreements may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.
2. **Lock-in.** There is currently little on offer in the way of tools and procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another, or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular cloud provider for service provision, especially if data portability, as the most fundamental aspect, is not enabled.
3. **Isolation failure.** Multi-tenancy, shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing, even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g., against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

4. **Compliance risks.** Investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud:
   a. if the cloud provider cannot provide evidence of their own compliance with the relevant requirements
   b. if the cloud provider does not permit audit by the cloud customer.

   In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved.

5. **Management interface compromise.** Customer management interfaces of a public cloud provider are accessible through the Internet, mediate access to larger sets of resources (than traditional hosting providers), therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
6. **Data protection.** Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider, thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities, the data controls they have in place, e.g., SAS70 certification.
7. **Insecure or incomplete data deletion.** When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies, the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.
8. **Malicious insider.** While usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include cloud provider system administrators and managed security service providers.

The risks listed above do not follow any specific order; they are just some of the most important cloud computing specific risks identified during the assessment. ENISA's report delves further into a more detailed analysis of specific risks in several categories such as policy, organizational risks, technical risks, legal risks and some risks not specific to the cloud.

ENISA's and Gartner's reports, while partly overlapping, also complement each other and together give a fair overview of risks that both, cloud service users and cloud service providers, may expect to face in the course of building a cloud economy.

Ironically, books on security sell poorly, whereas books on hacking into systems sell much better, a trend that is worrying when taking into account the increasing magnitude of these problems. Here is a sampling of titles that can be of use to interested reader who wants to extend his knowledge into the field of information security, especialy in areas discussed here:

- Challenges, approaches and solutions to risks of information security in computing systems: (Fagen, 1978), (Lerner *et al.*, 2002), (Cranor, 2005), (Winkel *et al.*, 2005), (Biskup, 2009), (Viega, 2009), (Wong and Yeung, 2009), (Arata, 2010), (Graham *et al.*, 2011), (Andress, 2011).
- Information security issues in contemporary distributed computing systems – Web 2.0., grid, cloud: (Mather, 2009), (Rittinghouse and Ransome, 2010), (Thuraisingham, 2011).
- Managing information security and associated risks: (Broder, 2006), (Tipton and Krause, 2008), (Arata, 2010), (Aven and Renn, 2010), (Vladimirov *et al.*, 2010), (Brotby, 2009), (Tiller, 2011).
- Identity, privacy and access control: (Benantar, 2005), (Windley, 2005), (Waldo *et al.*, 2007), (Mather, 2009), (Arata, 2010), (Nin, 2010), (Sileo, 2010), (Papacharissi, 2011).

While being aware of risks in itself is pointless unless we can do something about it, it follows that we must manage these risks. However, due to the asynchronous nature of the problem at hand we not only have to manage the risks, but we also have to build confidence in that the risks *are* being managed and that the transaction is trustworthy in itself if we follow certain rules including risk management. This, and more, is discussed in Section 4.

4. Trust and risk management

In his influential book (Fukuyama, 1995), Francis Fukuyama argued that public values, especially trust, shape the direction of national economies. Among other things, Fukuyama shows how trust reduces transactions costs, and ultimately, economic friction. Here, we will first give a brief overview of trust and its relation to confidence as it is seen from sociological standpoint. Then we will proceed to discuss the ways trust is seen in the realm of information technology. This would establish a background for thinking about a better use of trust and confidence concept to mitigate some risks in distributed computer architecture.

4.1 The importance of trust

Many authors have emphasized the importance of trust for achieving organizational success. The overview presented in (Six, 2005) shows that many see trust as necessary in contexts of high ambiguity and uncertainty, as well as in contexts of high complexity. Trust, on the one hand, can provide a sense of security that will help survival in these contexts, and on the other, it can help with the risk taking necessary for survival in complex environments. Trust, when present, is said to enhance the ability to change and to support, potentially radical, change. This is because trust is said to assist in learning, creativity and innovation. Furthermore, it is a lubricant for social relations which improves efficiency or, as John Locke declared, trust is ‘the bond of society’, the *vinculum societatis*.

Trust is also seen to foster and maintain cooperation, as it encourages information sharing, enriches relationships, increases openness and mutual acceptance, and enhances conflict resolution and integrative problem solving. The presence of trust, it has been argued, reduces the need for detailed contractual and monitoring devices, is thus important in governance and taking it one step further, in complex environments, detailed contracting and monitoring are often undesirable since they may constrain the scope and motivation for quality, for innovation based on individual variety and initiative. Trust can have extrinsic value, as a means to achieve social or economic goals, and it can have intrinsic value, as a dimension of relations that is valued for itself, as part of a broader notion of well-being or the quality of life. People may prefer, as an end in itself, to deal with each other on the basis of trust. One motive for doing this is to build confidence, which is discussed next.

4.2 Trust and confidence

We define trust as the willingness, in expectation of beneficial outcomes, to make one vulnerable to another based on a judgement of similarity of intentions or values, but here we want to emphasize that trust is based on social relations, group membership and shared values. Confidence is defined as the belief, based on experience or evidence, that certain future events will occur as expected. Both trust and confidence support cooperation. But whereas confidence has a specific performance criterion, trust is placed in the freedom of the other. In the case of trust, the other is free to act in ways that indicate shared values, regardless of whether specific acts are expected or not. In the case of confidence, the other must act in specifically expected ways.

The crucial point that is generally overlooked is the dependence of confidence on trust (O'Neill, 2004 as cited in Siegrist, 2007). We all describe within communities; we can't do otherwise. However, since our descriptions are linked to our communities, and accepted as justified only within them, we normally are not made aware of the dependence of the one upon the other – and the potential rejection of our descriptions within other communities. To take a very simple example, one might claim that one's confidence that the Earth will circle the sun is not based on a relation of trust. But one only has the idea of 'the Earth circling the sun' as a consequence of one's membership in a particular community. There is nothing given about that or any other description. This, of course, can become a serious matter when the descriptions one makes provoke more variable, contested effects on others than a description of the Earth's relation to the sun.

4.3 Trust and distributed computer system architecture

Within the realm of technology, trust and control have usually been associated with reliability, integrity (Smith, 2005) and correctness (Jayaswal and Patton, 2006) and were not seen as a separate issue until the arrival of complex computer-controlled systems. Computer science had initially approached trust, control from the perspective of security. Recognising that trust is not controllable, the security developed an elaborate structure of control, in an attempt to minimise elements of trust. However, more recently, the recognition of the fundamental nature of trust has been addressed in initiatives such as trusted computing, where individual devices are given assurance in their own configuration on the basis of a hardware-based root of trust. The need for a portable root of trust has also fuelled the creation and popularity of smart cards (Cofta, 2007).

In data communication, the understanding that trust precedes meaningful and secure communication has eventually led to the concept of trust management, the separate layer of interactions that lead to the creation and maintenance of trust relationships between communicating nodes, following e.g. business agreements, contractual dependence, personal relationship, etc. Pretty Good Privacy (PGP) has been exploring the area of peer-to-peer trust while Public Key Infrastructure (PKI) proposed the multi-stage model of trust (Biskup, 2009). More recently, Web Services Trust language (WS-Trust) has established itself as a standard within Service-Oriented Architecture (SOA), the potential foundation of Web 2.0 (Thuraisingham, 2010). Grid computing and pervasive computing environment have brought different challenges to trust management.

The need to effectively manage distributed computing systems has led to constructs such as trusted domains (several computers trusting each other's authentication capabilities) (Rittinghouse, 2010), trusted credentials (others' identities accepted without any further proof), trusted storage (storage space accessible only to selected users), trusted zones (privileged Internet address space) etc. In all these cases there is a notion of trust as essential yet different from actual cooperation or communication, something that requires special management practices. Usually, the ability to manage trust is granted to system administrators or users, in the expectation that the technical structure of trust will reflect trust in respective social relationships. Research on autonomous agents has liberated trust management from the need for an *a priori* trust, managed by the user or the administrator. Agents were vested with the ability to make and break the trust relationship (that can be more correctly called 'the relationship of confidence'), usually on the basis of past experience and through the process of learning, whether from direct interactions or from others' experience. Autonomous agents have brought the notion of imperfect trust (where trust is no longer a binary proposition), the problem of trust propagation and reasoning. The new approach to trust has also, unfortunately, revealed new threats to trust, usually in the form of attacks on reputation.

Interest in large systems, whether created by autonomous agents, *ad-hoc* networks or in any other way, required more specific instruments to discuss the reasoning about trust. Formalisation of trust proposes logical primitives, schemes that can be used in reasoning about trust. The formalisation of reasoning has led to the creation of several formal systems and supporting tools. Both reasoning and transitivity require trust and confidence to be qualified. The desire to measure trust and confidence generated significant amount of research.

From a more application-specific perspective, electronic commerce has used various metrics of trust to develop risk assessment, both for the seller, for the buyer. The commercial value of eBay's reputation system is widely known, and similar rating systems are used by other e-commerce sites. Collaborative filtering has been used to aid information search following the concept that trust is a qualified reliance on information, but as more automated systems moved into the area, collaborative filtering became the preferred solution for the recommendation. The needs of electronic commerce have stimulated the interdisciplinary approach to trust.

Another effect of the introduction of electronically mediated communication is the development of research in user trust in digital devices, e.g. in a form of web features that facilitate the creation of perceived trust, trust in information systems or in improvements of trust between people while communicating through a digital channel.

In a distributed computer system the establishment of trust typically includes specific administrative permissions and leverages cryptographically secure methods. These methods can establish identities, and provide various secure services to managed users. The full use of network services is reserved for managed users. These users have an identity on the network and are therefore trusted to interact with their piece of the network, which we will call 'cell', an organized collection of networked computers. By authenticating itself to the network and continually validating its authenticated status, this cell may become a trusted member of a network, which is also a cell, built on the same blueprint as the lower level cell.

Interested readers can find additional insight into the area of trust and confidence in the following literature:

- Intrinsic value of trust: (Blau, 1964), (Bradach, Eccles, 1989), (Gulati, 1995), (Nooteboom, 1996), (Powell, 1996), (Ryan, Oestreich, 1998), (Sako, 1998), (Marek, 2008), (Briggs, 2010).
- Trust is necessary in contexts of high ambiguity, uncertainty, and in contexts of high complexity: (Lewis, Weigert, 1985), (Shapiro, 1987), (Nooteboom, 1996), (Shaw, 1997), (Deering, Murphy, 1998), (Lane, 1998), (Nahapiet, Ghoshal, 1998), (Rousseau *et al.* , 1998), (Sako, 1998), (Senge *et al.*, 1999), (Costa, 2000), (Marek, 2008).
- How trust can provide a sense of security which will help survival in contexts of high ambiguity, uncertainty, and in contexts of high complexity: (McAllister, 1995), (Ellinor, Gerard, 1998), (Ryan, Oestreich, 1998), (Reina, Reina, 1999), (Senge *et al.*, 1999).
- How trust can help with risk taking necessary for survival in contexts of high ambiguity, uncertainty, and in contexts of high complexity: (Katzenbach *et al.*, 1995), (Shaw, 1997), (Lewis, 1999), (Reina, Reina, 1999), (Senge *et al.*, 1999), (Costa, 2000), (Marek, 2008).
- How trust enhances ability to change, supports radical change: (Argyris, 1970), (Katzenbach et al., 1995), (Shaw, 1997), (de Geus, 1997), (Deering, Murphy, 1998), (Ellinor, Gerard, 1998), (Ryan, Oestreich, 1998), (Reina, Reina, 1999), (Senge *et al.*, 1999), (Costa, 2000), (Marek, 2008).
- How trust assists in learning, creativity, innovation: (McAllister, 1997), (Shaw, 1997), (Zand, 1997), (Deering, Murphy, 1998), (Lane, 1998), (Lazaric, Lorenz, 1998), (Nahapiet, Ghoshal, 1998), (Rousseau *et al.*, 1998), (Ryan, Oestreich, 1998), (Sako, 1998), (Ghoshal, Bartlett, 1999), (Lewis, 1999), (Reina, Reina, 1999), (Senge *et al.*, 1999), (Costa, 2000), (Marek, 2008).
- Trust as a lubricant for social relations which improves efficiency: (Blau, 1964), (Fukuyama, 1995), (Hosmer, 1995), (Deering, Murphy, 1998), (Hollis, 1998).
- Trust fosters, maintains cooperation, as it encourages information sharing, enriches relationships, increases openness, mutual acceptance, enhances conflict resolution, integrative problem solving: (Shapiro, 1987), (Katzenbach *et al.*, 1995), (Mayer *et al.*, 1995), (Ross, LaCroix, 1996), (Wheatley, Kellner-Rogers, 1996), (Shaw, 1997), (Zand, 1997), (Deering, Murphy, 1998), (Elangovan, Shapirio, 1998), (Lane, 1998), (Rousseau *et al.*, 1998), (Ryan, Oestreich, 1998), (Tsai, Ghoshal, 1998), (Whitener *et al.*, 1998), (Zaheer *et al.*, 1998), (Ghoshal, Bartlett, 1999), (Lewis, 1999), (Reina, Reina, 1999), (Senge *et al.*, 1999), (Costa, 2000), (Marek, 2008), (Cofta, 2007).
- Trust applied to data transfer, storage in public networks and information systems: (Robinson *et al.*, 2005), (Lu and Tsudik, 2010), (Dong and Dulay, 2010), (Kellermann *et al.*, 2010), (Ma *et al.*, 2010), (Cornelis and De Cock, 2011).
- Trust, information security and risk management: (Benantar, 2005), (Siegrist, 2005), (Veeningen *et al.*, 2010), (Muller, 2010), (Khoury and Tawbi, 2010), (Crampton, 2010), (Ballardin and Merro, 2010), (Kamil and Lowe, 2010).

Next, we propose a concept of *multilevel cell distributed computer system* architecture capable of providing enhanced trust services and increased confidence to both cloud providers and cloud consumers, thus providing a foundation for future development of cooperation on global network, with better management and mitigation of risks.

5. Multilevel cell distributed computer system architecture

In the realm of distributed computer systems, such as Internet, trust and confidence are relations that could be established between digital, virtual entities inhabiting this realm. Virtual entities could represent real persons as well as technical resources (services). In order to make use of trust and confidence to promote better cooperation, we need a reliable identity management system capable of collecting, interpreting and representing social information about virtual entities, among other things. Social networks are building on this idea but they tend to centralize information. Every network builds its own set of information about entities, which gives rise to the kind of problems explained in the introduction of this chapter. Also, they lack appropriate interpreting functions that could provide measures of social trust needed to establish confidence.

To address such issues we devised a *cell* as a basic building block of distributed computer systems infrastructure. Cell is a self-contained computer system with clearly established boundaries, capable of communicating with other such systems. The smallest cell could be a single physical computer, although it can host several virtual entities, persons or services. A cell can be built from several computers dedicated to various cell functions. Several cells can be connected together to form a larger entity which represents itself as a cell to outer world, providing the same cell functions. It is thus possible to build a *multilevel cell distributed computer system*.

Cells need to provide many functions for their operation and cooperation within a distributed system. These functions have to be built upon certain design principles we established as a foundation to proposed architecture. We will here mention only those principles (Lerner *et al.*, 2002) that support our discussion regarding trust and confidence:

- computers associated with a cell direct all traffic between entities to flow unconditionally through its edge gateways (interconnection computers);
- all entities that establish a relationship with a cell must register with the cell;
- all traffic passing through the cell must be authenticated;
- the cell tracks all active entities.

Cell-based distributed system architecture is a development from the architectural concept based on communicating proxies, as described by (Lerner *et al.*, 2002). This is expanded on next.

5.1 Physical cell architecture

Although all functions can be implemented in single computer, it is recommended to implement different functional elements into different computers. Having this in mind we will call these computers, similarly: *access computer*, *interconnection computer*, *storage computer* and *service computer*. These computers comprise building blocks of the cell's internal architecture, as shown by Figure 3.

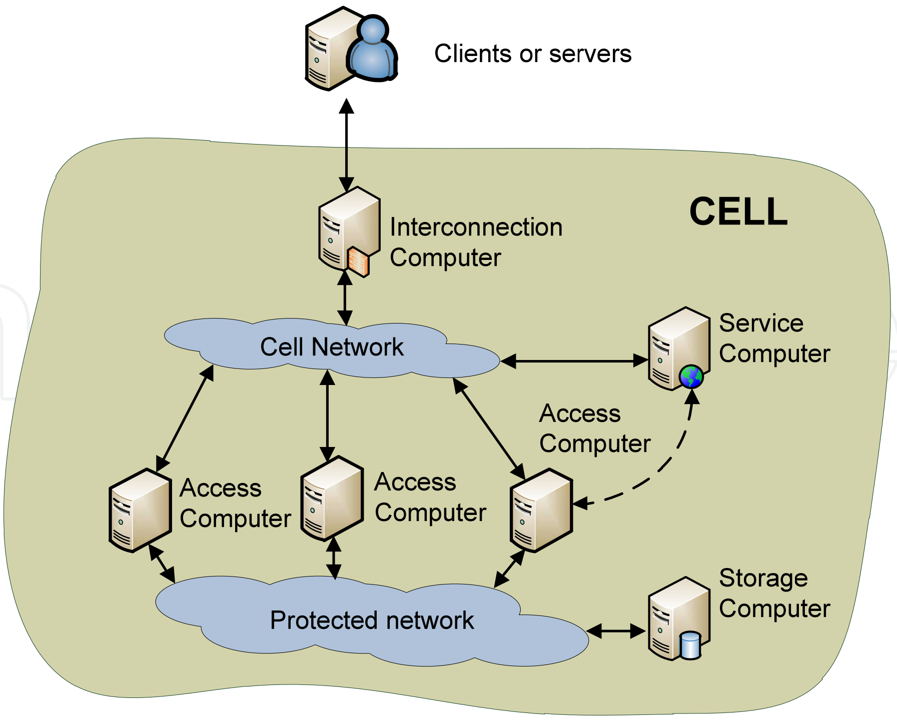


Fig. 3. Basic cell architecture

Interconnection computers enable communication with other networks and provide security boundary for the cell. They also run several other security related tasks such as registration, identification, authentication, accreditation, encryption/decryption, etc.

Service computers are, by their functions, general servers. They provide services to other computers, internal or external to the cell. Service computer can be connected to the cell network or directly to access computer.

Access computers are, by their function, proxy computers with some extended functionality. They are characterized by having at least two network interfaces. One interface connects access computer into the protected network that enables them to communicate with each other. Other interfaces connect access computers with external computers (clients, servers or other cells) through the cell network and interconnection computer.

Storage computers are essentially database servers. They provide services, related to databases stored on them, to other cell computers, but only through access computers. Therefore data stored in the cell are not directly reachable by the external computers.

Internally, cell has two networks: *cell network* and *protected network*. Cell network is semi-public network into which external computers (clients, servers or other cells) can enter through interconnection computer, so as to gain access to service computer or access computer. Interconnection computers and cell's security services protect this network from unauthorized access by external systems.

Protected network is unreachable for external computers, and only access computers can connect into it, in order to access the cell's data contained there on the storage computers which are also attached to the protected network. No traffic generated externally to the cell is allowed into this network.

We can also look at the physical cell architecture from a functional point of view. This view will show us four functional elements: interconnection, access, storage and service. Remember that a cell could be hosted on the single computer so these functional elements need not be implemented on physically different devices.

Functionally, we can have more views of the cell. Let's look at the cells placed at various levels of the distributed computer system hierarchy. Depending of their functional level, a cell will have different emphasis on various functions within it, as discussed in the next section.

5.2 Functional cell levels

Basic functional cell level is network. Cell in this level is called *network cell*. Network cell is based on locality of computers which constitute the cell. It is supposed that computers in the network cell all are contained in single building or several closely placed buildings, interconnected by private, physically secured network. Network cell centralizes functions such as traffic management, network management, quality of service management, messaging, etc.

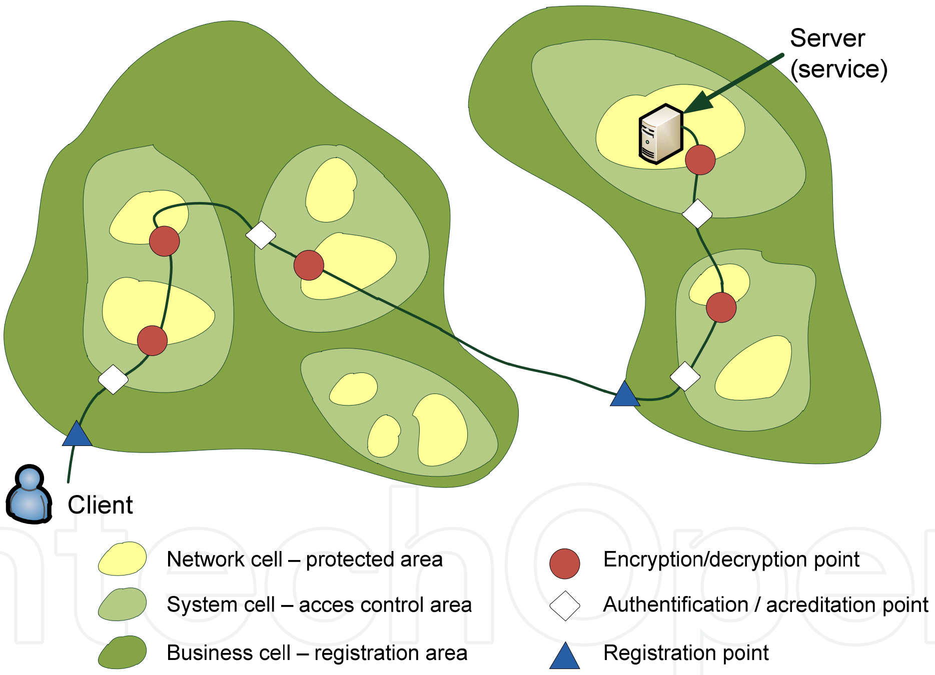

Server
(service)
Client
Network cell – protected area
System cell – acces control area
Business cell – registration area
Encryption/decryption point
Authentification / acreditation point
Registration point

Fig. 4. User query traversing a multilevel cell distributed computer system

Network cells are being connected together to form a *system cell*. If communication between network cells is not local, protected, there should be encryption/decryption function built into interconnecting computers. System cell centralizes functions of user identification, authentication, and accreditation.

To implement connection function efficiently, it should be founded on three general principles: *knowledge abstraction*, *lazy calculation*, and *multiplication of data about clients and servers*. All three principles are supported by cell architecture described here.

Knowledge abstraction supposes construction of abstract model for unified representation of servers and clients in our computer system. In the first step, the notion of server (physical entity providing a certain service) is replaced by more abstract term service (service itself) which cloaks physical characteristics of server computer. Thus, instead of client/server architecture, we are considering client/service architecture. This abstraction is especially convenient in modelling of distributed systems based on non-connection protocols. In such systems a client addresses a service, not a physical object. It has to be noted also that distinction between client and service is temporary and lasts only through single transaction. In the very next transaction roles could be reversed. Using knowledge abstraction we are able to disregard this difference at the model level.

Lazy calculation of object characteristics supposes that neither all objects, nor all their attributes, are at every moment present locally in all cells of distributed architecture. Only when objects' characteristic is explicitly referenced the system will contact other cells to retrieve the needed information. This principle is supported by institution of global catalogue which collects all objects but only with some subset of attributes.

Multiplication of data about clients and servers is achieved by partitioning and replicating objects into other cells. Replication topology and schedule should be designed carefully to optimize network traffic.

Cell architecture also supports efficient network traffic management, based on data replication as well as multiplication and distribution of functions. Network cell manages and monitors traffic, sends massages to computers or group of computers, measures and allocates bandwidth, etc. System cell replicates system and server data, and distributes control and administrative jobs. Business cell redirects network traffic, based on information in registration databases, internally or towards other cells.

While majority of connection, traffic management functions are performed by network and system cells, fundamental business cell purpose is to provide support to information system By executing many of monitoring, security and administrative functions, business cell simplifies server and client operation and makes their connection efficient.

5.3 Functional cell architecture

A cell is a fundamental building block of a distributed computer system. Single cell by itself also represents a distributed computer system, so it has to contain all functionalities of a whole distributed system. Thus by describing single cell functionality we are describing the functionality of the whole proposed distributed system.

Cell's basic functional structure is shown by Figure 5. In relation to Figure 3, showing types of networks and computers comprising a cell, Figure 5 emphasizes systems and services that implement cell functionality. Functions and services can be situated on one or more computers shown on Figure 3, and vice versa – several functions can be provided by single computer. Typical function and computer mapping between Figure 3 and Figure 5 might be as follows:

- *Interconnection computers* implement *security perimeter control* function (they are essentially firewalls);

- *Service computers* implement most of system functions – *identity management, certificate, keys management, business process orchestration, service publishing, message transfer, management, documents transfer, management, mobile services, cell management;*
- *Access computers* implement *application services;*
- *Storage computers* implement *database services*, as well as *legacy applications* where appropriate.

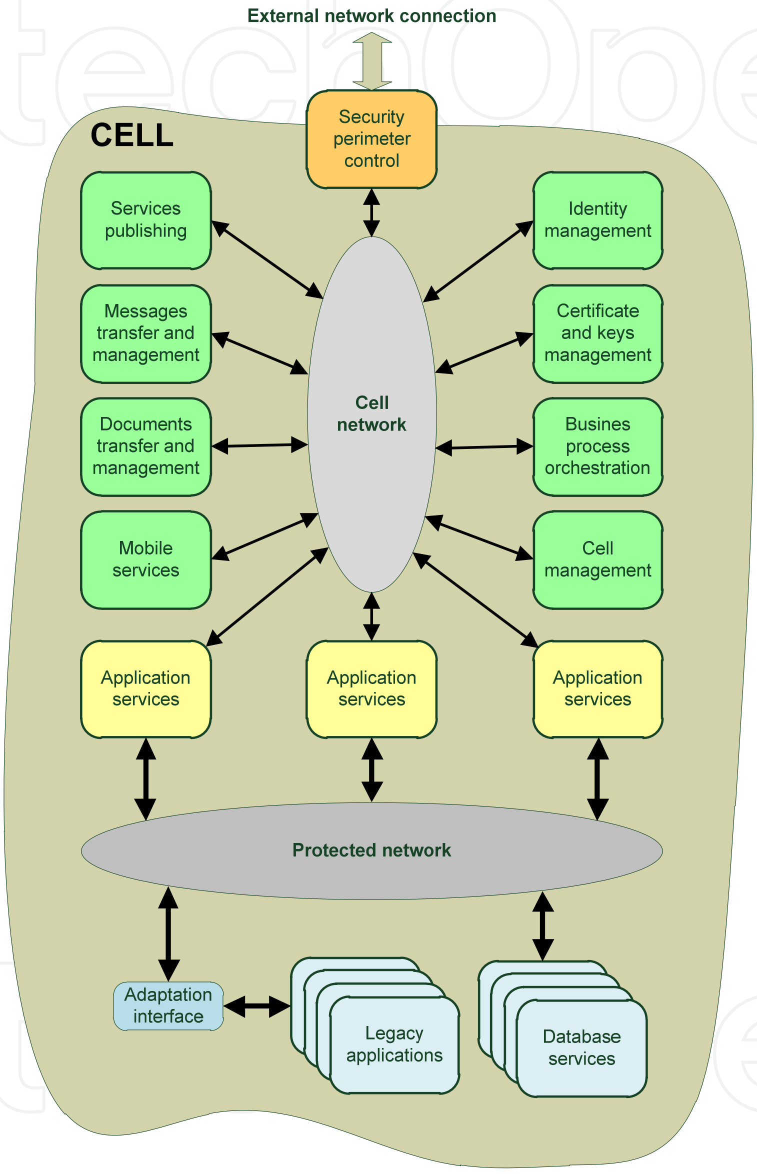


Fig. 5. Functional cell architecture

The key cell function providing support to promote trust in our proposed architecture is *identity management*. In a 'real world' an identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons. In cell architecture term 'identity' is extended to every identifiable object within distributed computer system, which may include persons as well as services. *Digital identity* is a digital representation of a 'real world' object. Digital identity is implemented as data structure characterizing the entity.

Besides basic data necessary for addressing (location and identification) identity can encompass data for other purposes such as authentication, accreditation, administration, brokerage, certification, provisioning, etc. In our model, identity data also include components that collect trust related information.

Cell's identity management is a framework within which digital identities are managed in the distributed computer system. Digital identity management comprises two parts: a) digital identity repository (directory) implemented as distributed, partitioned and replicated database, and b) set of operations on identity data. Full set of digital identity data is situated in a cell where there is an ownership relation on them, either original cell where identity was created or a cell where identity ownership was transferred.

Identity management subsystem is a hierarchical set of functions (Vukovic, 2011), consisting of:

- **Identity administration** – establishes digital identity's compliance with business processes:
  - *Existence* – digital identity establishment within the cell;
  - *Context* – managing information about digital identity's working environment; collection of trust related information belongs here;
  - *Provisioning* – connects digital identity dynamically with various tools administered to it through its life cycle.
- **Community management** – promotes cooperation between various groups of digital identities, i.e. digital communities:
  - *Authentication* – checks and confirms authenticity of digital identity's data, supports privacy and confidentiality;
  - *Authorization* – gives permission to access and utilize distributed resources and services; uses trust related data to determine level of confidence;
  - *Rendezvous* – establishes an appropriate level of cooperation between digital identities based on calculated trust and confidence information.
- **Identity integration** – makes a holistic view of identity data and establishes a consistent digital identity representation for other cells:
  - *Ownership* – while subsets of identity data may be replicated throughout distributed system, ownership of original data must be maintained and remain under sole control of primary owner;
  - *Brokerage* – exchanges information about digital identities between cells; collects trust related data when applicable;
  - *Connection* – establishes connections between cells for the purpose of identity data exchange.

Subset of digital identity data is available to other cells, depending on a level of trust needed for a digital identity to interact with cell's services. This subset of data is a digital identity's *virtual presentation*. Cell's identity management function keeps this subset at a necessary minimum to optimize privacy and minimize traffic.

6. Cooperation in multilevel cell distributed computer systems

In this section we will discuss the idea, stated in the introduction, that multilevel cell architecture can leverage trust relationship building between virtual entities on Internet, thus raising the level of confidence, resulting in more cooperation (i.e. business). For this purpose we will use the Trust, Confidence and Cooperation (TCC) model, described in (Siegrist, 2007).

The TCC model is designed to serve several useful purposes. The first is unification. It provides a framework within which all expressions of trust and confidence can be interpreted, related to one another. The second is specification. To a greater extent than available alternatives, it identifies the basic psychological processes involved in judgements of trust and confidence. The third is clarification. At the centre of the TCC model is an explicit account of the interaction between trust and confidence, a major source of confusion in other approaches. The final purpose is generation of new insights. By unifying and bringing more specificity and clarity to the understanding of trust and confidence, the TCC model points to potentially fruitful connections with other areas of social, psychological and applied research, and suggests novel research hypotheses.

The TCC model of cooperation postulates that trust is based on social relations and on shared values. Shared values can be measured in many different ways. In empirical studies, trust can be indicated variously by measures of in-group membership, morality, benevolence, integrity, inferred traits, intentions, fairness and caring. All of these, we will argue, can be taken to mean good intentions relative to those of the trusting person shared values.

As defined in (Siegrist, 2007) the model identifies constituent (in-coming) and product (out-going) elements, but does not specify how the former are combined to produce the latter. This allows for model to be mapped to functions of various systems, provide a basis for evaluation of how these functions contribute to cooperation. Elements of TCC model, as described in (Siegrist, 2007) are the following:

1. *Perceived amplitude of morality/performance information*: the judged degree to which the given information has morality/performance implications.
2. *Perceived valence of morality/performance information*: the judged degree of positivity/ negativity of the given information.
3. *Attributed values/performance*: the values/performance attributed by the observer to the other.
4. *Active values/active performance history*: in the case of values, these are the values that are currently active for the observer – which may be the product of existing social trust relations. In the case of performance, this is whatever history of relevant performance that is currently active for the observer.
5. *General trust/general confidence*: general trust is defined and discussed in previous sections. General confidence is the performance-based counterpart of the values-based general trust: the belief that things, in general, are under control, uncertainty is low and events will occur as expected.
6. *Value similarity/perceived performance*: value similarity is the judged similarity between the observer's currently active values and the values attributed to the other. Perceived performance is the observer's interpretation of the other's performance.
7. *Social trust/confidence*: these elements are defined and discussed in previous sections.
8. *Cooperation*: any form of cooperative behaviour between a object and another object or group of objects.

The application of the TCC model to evaluate the ability of cell architecture to enhance cooperation by utilizing trust and confidence information into identity management, is shown in Figure 6. The elements of the TCC model are aligned in parallel pairs for trust and confidence. Upper row of elements deals with trust, and lower row of elements deal with confidence. Both rows are combined at the right to produce a cooperation of a certain level.

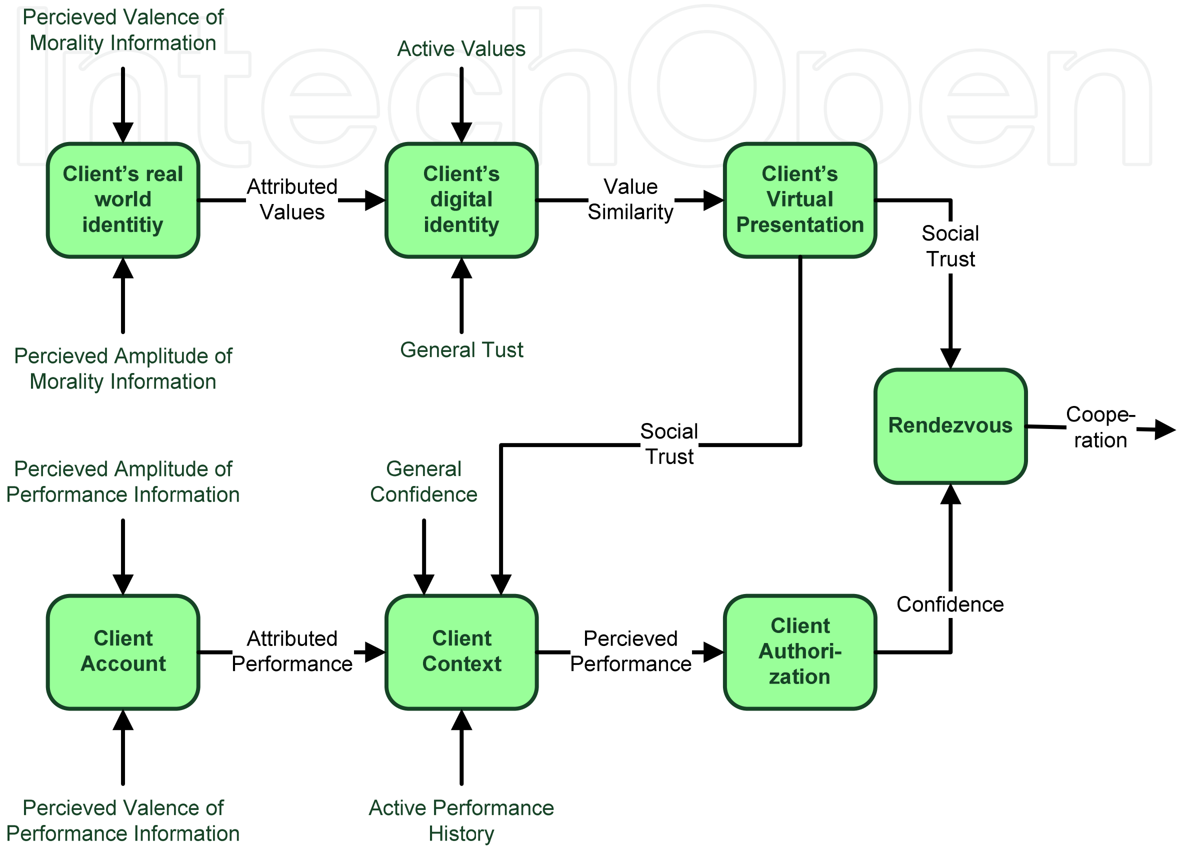

Percieved Valence of Morality Information
Active Values
Client's real world identitiy
Attributed Values
Client's digital identity
Value Similarity
Client's Virtual Presentation
Social Trust
Percieved Amplitude of Morality Information
General Tust
Rendezvous
Coope-ration
Social Trust
Percieved Amplitude of Performance Information
General Confidence
Client Account
Attributed Performance
Client Context
Percieved Performance
Client Authori-zation
Confidence
Percieved Valence of Performance Information
Active Performance History

Fig. 6. TCC model of cooperation in multilevel cell distributed system

Client's real world identity, client's physical and social 'self', is attributed with perceived valence and amplitude of morality information. These attributes represent client's morality as viewed by the community, and attributed values are maintained within client's digital identity, where they are combined with active values and general trust, to obtain a trust measure of digital identity. Based on the value similarity, depending on specific application needs, cell's identity management function will establish client's virtual presentation with corresponding social trust level in a domain of application.

At the service (server) cell there is an object called client account, a set of data containing information about client identity, as well as perceived valence and amplitude of performance information. This means that service provider is collecting past performance data about client as a basis of confidence, thus obtaining attributed performance info to the client context where it is combined with general confidence, social trust and active performance history. Resulting measure of perceived performance is fed to the client authorization where the appropriate level of confidence is established to the client to utilize specific resources.

At far right, value of social trust presented by client's virtual presentation and service provider's confidence expressed in client authorization are fed to rendezvous function to enable cooperative behaviour between client and service. Rendezvous function also checks the authenticity of cooperating parties.

Let's illustrate this process with the case of Cory Doctorow's inability to buy some music from Amazon, described in the introduction.

Trust: Cory Doctorow is a public person, known worldwide by his writing, public addresses, activism, etc. His morality information perceived valence is positive with quite high amplitude, though we will not try to give any exact measures here and now. From this information we can derive attributed values and input them into Doctorow's digital identity. Based on a value similarity between the cell's currently active values and the values attributed to the Doctorow's digital identity, system is able to create virtual presentation of Doctorow's digital identity, for this application of buying online music, as a man who will most likely pay all his expenses in time.

Confidence: Amazon's web shop keeps information about Doctorow's digital identity in form of a client account record. There it keeps various information about Doctorow's performance perceived by observing his digital identity's behaviour on Amazon web site, creating attributed performance as an input to the client context. Here the attributed performance data will be combined with Amazon's active performance history, general confidence and Doctorow's social trust level (according to lazy calculation principle, social trust will be included into calculation only when needed and available, e.g. when Doctorow signs into Amazon web shop). This yields the perceived performance information which will serve as a basis to authorize Doctorow to use certain resources, in this case to buy some music, thus expressing confidence that Doctorow's credit card information is valid and there is no risk of fraud.

Rendezvous: when Doctorow actually signs into the Amazon web shop and successfully authenticates his digital identity, rendezvous function combines his virtual presentation social trust information with confidence information on Amazon web site and enables transaction to proceed – Doctorow to download some music, and Amazon to charge his credit card with the proper amount.

Because the trust-confidence relation is established on the basis of perceived morality and performance information, instead of locality information (origin of credit card, IP address, etc.) cooperation may be independent of client or service location, i.e. Mr. Doctorow could buy music from any location on the planet, equally successfully from Amazon US, Amazon UK, or any other Amazon store.

7. Closure

Most of the functions of cells can be implemented with ready available software, although some adaptations may be needed such as, for example, inclusion of trust and confidence data with appropriate calculations into the identity management solution.

Conceptually, cell based architecture requires a global set of standards and compliance. Compliant and certified applications will enable network operators to achieve better account control and increased network traffic.

To enable cooperation of different components in a distributed computer system, unified interface between these components should be devised and implemented. Unified interface defines common data transfer formats and commands, using standardized protocols to achieve data independence. To support the asynchronous nature of the cell architecture, use of connectionless protocols is preferred.

Multilevel cell distributed computer system architecture has many implications to various technological and social aspects of distributed systems, especially Internet, which are not discussed here. We have discussed here only the ability of multilevel cell distributed architecture to leverage cooperation in on-line economy by including trust and confidence information into its identity management system. We do believe that cell based architecture, implemented into Internet, may offer an increased control over user identities yet support their mobility, thus reducing the risks of identity theft and related frauds, securing service providers against loss of confidential data, financial risks that may follow.

With cell architecture, network service providers can reduce cost, ease the entry into new markets, and be the vehicle for key partnerships with software vendors, content providers, and other businesses. But, the main development here is the ability to establish trust relationships not only among people represented by their digital identities, but also among digitally identified computing services in a distributed system. This could lead to a whole new practice of doing business online. We could envisage digital services trusted to negotiate with each other with confidence to reach the optimal agreement for all parties involved. For example, internet service provider infrastructure cells could negotiate optimal cost of bandwidth with cells holding long-haul data services. This could be done in seconds thus providing a very effective response to system dynamics, reducing risks due to interruptions of long-haul services.

Of course, this kind of infrastructure behaviour is yet to be extensively researched. Nevertheless, the interaction dynamics in presence of cells that intentionally change their behaviour based on trust relationship does appear as a promising and interesting research direction and worthy of further development.

8. Acknowledgment

This work has been supported, in more ways than just financially, by KING ICT Ltd., Croatia, http://www.king-ict.hr

9. References

Androulaki, E., Bellovin, S. (2009). *An Anonymous Credit Card System, in Trust, Privacy and Security in Digital Business, Proceedings of 6th International Conference, TrustBus 2009*, ISBN 978-3-642-03747-4, Linz, Austria, September 2009

Andress, J. (Ed.). (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Syngress, ISBN 978-1-59749-653-7, Waltham MA, USA

Arata Jr., M. J. (2010). *Identity Theft For Dummies*, Wiley Publishing Inc., ISBN: 978-0-470-56521-6, Hoboken NJ, USA

Aven, T., Renn, O. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications*, Springer-Verlag, ISBN 978-3-642-13925-3, Berlin, Germany

Ballardin, F., Merro, M. (2010). *A Calculus for the Analysis of Wireless Network Security Protocols*, in *Formal Aspects of Security and Trust, Revised selected papers of 7th International Workshop, FAST 2010*, ISBN 978-3-642-19751-2, Pisa, Italy, September 16-17, 2010

Benantar, M. (2005). *Access Control Systems: Security, Identity Management and Trust Models*, Springer Science + Business Media, ISBN 978-0-387-27716-5, New York NY, USA

Biskup, J. (2009). *Security in Computing Systems: Challenges, Approaches and Solutions*, Springer Verlag, ISBN 978-3-540-78441-8, Berlin, Germany

Blau, P.M. (1964). *Exchange, Power in Social Life*, Transaction Publishers, ISBN 978-0-887-38628-2, New York NY, USA

Bradach, J.L., Eccles, R. G. (1989). Price, authority, trust: from ideal types to plural forms, *Annual Review of Sociology*, Vol. 15, Aug 1989, pp. 97–118, ISSN 0360-0572

Briggs, P., (2010). *The Evolution of Trust*, in *Trust Management V, Proceedings of 5th IFIP WG 11.11 International Conference, IFIPTM 2011*, ISBN , Copenhagen, Denmark, June 29 - July 1, 2011, (IFIP Advances in Information, Communication Technology)

Broder, J. F. (2006). *Risk Analysis, the Security Survey*, Butterworth-Heinemann, ISBN 978-0-7506-7922-0, Oxford, UK

Brodkin, J. (2008). *Gartner: Seven cloud-computing security risks*, In: InfoWorld, 2011-08-16, Available from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1

Brotby, W. K. (2009). *Information security governance: a practical development and implementation approach*, John Wiley & Sons, ISBN 978-0-470-13118-3, Hoboken NJ, USA

Catteddu, D., Hogben, G. (Eds.). (2009). *Cloud Computing: Benefits, risks and recommendations for information security*, European Network, Information Security Agency (ENISA), Retrieved from http://www.enisa.europa.eu/act/rm/ files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Cofta, P. (2007). *Trust, Complexity and Control: Confidence in a Convergent World*, John Wiley & Sons Ltd, ISBN 978-0-470-06130-5, The Atrium, Southern Gate, Chichester, England

Costa, A.C. (2000). *A Matter of Trust: Effects on the Performance, Effectiveness of Teams in Organizations,* dissertation, University of Tilburg

Crampton, J. (2010). *Cryptographic Enforcement of Role-Based Access Control*, in *Formal Aspects of Security and Trust, Revised selected papers of 7th International Workshop, FAST 2010*, ISBN 978-3-642-19751-2, Pisa, Italy, September 16-17, 2010

Cranor, L. F., Garfinkel S. (2005). *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly Media, ISBN 0-596-00827-9, Sebastopol CA, USA

Deering, A., Murphy, A. (1998). *The Difference Engine: Achieving Powerful and Sustainable Partnering*, Gower, ISBN-13: 978-0-566-08048-7, Aldershot, England

Denison, D. R. (1996). What is the difference between organizational culture, organizational climate? A native's point of view on a decade of paradigm wars, *Academy of Management Review*, Vol. 21, No. 3, Oct 1996, pp. 619–54, ISSN 0363-7425

Dong, C., Dulay, N. (2010). *Longitude: A Privacy-Preserving Location Sharing Protocol for Mobile Applications*, in *Trust Management V, Proceedings of 5th IFIP WG 11.11 International Conference, IFIPTM 2011*, ISBN , Copenhagen, Denmark, June 29 - July 1, 2011, (IFIP Advances in Information, Communication Technology)

Elangovan, A.R., Shapiro, D.L. (1998). Betrayal of trust in organizations, *Academy of Management Review*, Vol. 23, No. 3, Jul 1998, pp. 547–566, ISSN 0363-7425

Ellinor, L., Gerard, G. (1998). *Dialogue: Rediscover the Transforming Power of Conversation*, John Wiley, ISBN 978-0-471-17466-0, New York NY, USA

Fagen, M. D. (Ed.). (1978). *A History of engineering and science in the Bell System: National Service in War, Peace (1925 - 1975)*, Bell Telephone Laboratories, ISBN 978-0-932-76400-3, New York NY, USA

Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, ISBN 978-0-684-82525-0, New York NY, USA

Georgantas, N. et al. (2010). *A Coordination Middleware for Orchestrating Heterogeneous Distributed Systems*, in *Advances in Grid and Pervasive Computing, Proceedings of 6th International Conference, GPC 2011*, ISBN 978-3-642-20753-2, Oulu, Finland, May 11-13, 2011

Geus, A. de (1997). *The Living Company: Habits for Survival in a Turbulent Business Environment*, Harvard Business Press, ISBN-13: 978-1-578-51820-3, Cambridge MA, USA

Ghoshal, S., Bartlett, C.A. (1999). *The Individualized Corporation: A Fundamentally New Approach to Management*, Harper Paperbacks, ISBN 978-088-7-30831-4, New York NY, USA

Governor, J., Hinchcliffe, D., Nickull, D. (2009). *Web 2.0 Architectures*, O'Reilly Media, ISBN 978-0-596-51443-3, Sebastopol CA, USA

Graham, J., Howard, R., Olson, R. (2011). *Cyber Security Essentials*, Auerbach Publications, ISBN 978-1-4398-5126-5, Boca Raton FL, USA

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances, *Academy of Management Journal*, Vol. 38, No. 1, Feb 1995, pp. 85–112.

Hollis, M. (1998). *Trust within Reason*, Cambridge University Press, ISBN 978-0-521-58681-8, Cambridge, UK

Hosmer, L.T. (1995). Trust: the connecting link between organizational theory and philosophical ethics, *Academy of Management Review*, Vol. 20, No. 2, Apr 1995, pp. 379–403,

Jayaswal, B. K., Patton, P. C. (2006). *Design for Trustworthy Software: Tools, Techniques, and Methodology of Developing Robust Software*, Prentice Hall, ISBN 978-0-13-187250-9, Upper Saddle River NJ, USA

Kamil, A., Lowe, G. (2010). *Understanding Abstractions of Secure Channels*, in *Formal Aspects of Security and Trust, Revised selected papers of 7th International Workshop, FAST 2010*, ISBN 978-3-642-19751-2, Pisa, Italy, September 16-17, 2010

Katzenbach, J.R. (1995). *Real Change Leaders*, Crown Business, ISBN 978-0-812-92923-2, New York NY, USA

Kellermann, B., Potzsch, S., Steinbrecher, S. (2010). *Privacy-Respecting Reputation for Wiki Users*, in *Trust Management V, Proceedings of 5th IFIP WG 11.11 International Conference, IFIPTM 2011*, ISBN , Copenhagen, Denmark, June 29 - July 1, 2011, (IFIP Advances in Information, Communication Technology)

Khoury, R., Tawbi, N. (2010). *Corrective Enforcement of Security Policies*, in *Formal Aspects of Security and Trust, Revised selected papers of 7th International Workshop, FAST 2010*, ISBN 978-3-642-19751-2, Pisa, Italy, September 16-17, 2010

Lane, D., Maxfield, R. (1995). *Foresight, complexity and strategy*, Santa Fe Institute, Working Paper 95-12-106, Dec 1995, Sante Fe NM, USA

Lazaric, N., Lorenz, E. (1998). The learning dynamics of trust, reputation and confidence, in *Trust and Economic Learning*, Lazaric, N., Lorenz, E. (Eds.). pp. 1–20, Edward Elgar Publishing, ISBN 978-1-858-98460-5, Cheltenham, UK

Lerner, M.; Vanecek, G. ; Vidovic, N. & Vrsalovic, D. (2002). *Middleware Networks: Concept, Design and Deployment of Internet Infrastructure,* Kluwer Academic publishers, ISBN 0-792-3784-7, New York NY, USA

Lewis, J.D., Weigert, A. (1985). Trust as a social reality, *Social Forces*, Vol. 63, No. 4, June 1985, pp. 967–984, ISSN 0037-7732

Lu, Y., Tsudik, G. (2010). *Enhancing Data Privacy in the Cloud*, in *Trust Management V, Proceedings of 5th IFIP WG 11.11 International Conference, IFIPTM 2011*, ISBN , Copenhagen, Denmark, June 29 - July 1, 2011, (IFIP Advances in Information, Communication Technology)

Ma, Y., Abie, H., Skramstad, T., Nygard, M. (2010). *Assessment of the Trustworthiness of Digital Records*, in *Trust Management V, Proceedings of 5th IFIP WG 11.11 International Conference, IFIPTM 2011*, ISBN , Copenhagen, Denmark, June 29 - July 1, 2011, (IFIP Advances in Information, Communication Technology)

Marek, K. (2008). *Trust: Self-Interest and the Common Good*, Oxford University Press, ISBN 978–0–19–921791–5, New York NY, USA

Mather, T., Kumaraswamy, S., Latif, S. (2009). *Cloud Security and Privacy*, O'Reilly Media, ISBN 978-0-596-80276-9, Sebastopol CA, USA

Mattern, T., Woods, D. (2006). *Enterprise SOA: Designing IT for Business Innovation*, O'Reilly Media, ISBN 0-596-10238-0, Sebastopol CA, USA

Mayer, R. C., Davis, J. H., Schoorman, F. D. (1995). An integrative model of organizational trust, *Academy of Management Review*, Vol. 20, No. 3, Aug 1995, pp. 703–34, ISSN 0363-7425

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations, *Academy of Management Journal*, Vol. 38, No. 1, 1995, pp: 24–59, ISSN 0001-4273

McAllister, D. J. (1997). The second face of trust: reflections on the dark side of interpersonal trust in organizations, *Research on Negotiation in Organizations*, Vol. 6, (Jan 1997). pp. 87–111, ISSN 1040-9556

Muller, T., (2010). *Semantics of Trust*, in *Formal Aspects of Security and Trust, Revised selected papers of 7th International Workshop, FAST 2010*, ISBN 978-3-642-19751-2, Pisa, Italy, September 16-17, 2010

Nahapiet, J., Ghoshal, S. (1998). Social capital, intellectual capital, the organizational advantage, *Academy of Management Review*, Vol. 23, No. 2., May 1998, pp. 242–66, ISSN 0363-7425

Nin, J., Herranz, J. (Eds.). (2010). *Privacy and Anonymity in Information Management Systems*, Springer, ISBN 978-1-84996-237-7, London, UK

Nooteboom, B. (1996). Trust, opportunism and governance: a process, control model, *Organization Studies*, Vol. 17, No. 6, Nov 1996, pp. 985–1010, ISSN 0170-8406

Papacharissi, Z., (Ed.). (2011). *A Networked Self: Identity, Community and Culture on Social Network Sites*, Routledge, ISBN13: 978-0-415-80180-5, New York NY NY, USA

Powell, W. W. (1996). Trust-based forms of governance, in *Trust in Organizations: Frontiers of Theory, Research*, Kramer, R.M., Tyler, T.R. (Eds.). pp. 51–67, Sage Publications, ISBN 978-0 803-95740-4, Thousand Oaks CA, USA

Preve, N. P. (Ed.). (2011). *Grid Computing: Towards a Global Interconnected Infrastructure*, Springer-Verlag, ISBN 978-0-85729-675-7, London, UK

Puder, A., Römer, K., Pilhofer, F. (2006). Distributed systems architecture: a middleware approach, Morgan Kaufmann, ISBN 978-1-55860-648-7, San Francisco CA, USA

Reese, G. (2009). *Cloud Application Architectures: Building Applications, Infrastructure in the Cloud*, O'Reilly Media, ISBN 978-0-596-15636-7, Sebastopol CA, USA

Reina, D. S., Reina, M.L. (1999). *Trust, Betrayal in the Workplace: Building Effective Relationships in Your Organization*, Berrett-Koehler, ISBN 1-57675-377-8, San Francisco CA, USA

Rittinghouse, J. W., Ransome, J. F. (2010). *Cloud Computing: Implementation, Management, and Security*, CRC Press, ISBN 978-1-4398-0680-7, Boca Raton FL, USA

Robinson, P., Vogt, H., Wagealla, W. (Eds.). (2005). *Privacy, security and trust within the context of pervasive computing*, Springer Science + Business Media, ISBN 0-387-23462-4, Boston, USA

Rousseau, D. M., Sitkin, S. B., Burt, R. S., Camerer, C. (1998). Not so different after all: a cross-discipline view of trust, *Academy of Management Review*, Vol. 23, No. 3, Sep 1998). pp. 393–404.

Ryan, K., D.K. Oestreich (1998). *Driving Fear out of the Workplace: Creating the High-trust, High-performance Organization*, Jossey-Bass, ISBN 978-0-787-93968-7, San Francisco CA, USA

Sako, M. (1998). Does trust improve business performance?, in *Trust within and between Organizations: Conceptual Issues, Empirical Applications*, Lane, C., Bachmann, R. (Eds.). pp. 88–117, Oxford University Press, ISBN 978-0-199-24044-9, USA.

Senge, P. M., Kleiner, A., Roberts, C., Ross, R., Roth, G., Smith, B. (1999). *The Dance of Change*, Crown Business, ISBN 978-0-385-49322-2, New York NY, USA

Serpanos, D., Wolf, T. (2011). *Architecture of Network Systems*, Morgan Kaufmann, ISBN 978-0-12-374494-4, Burlington MA, USA

Shapiro, S. P. (1987). The social control of impersonal trust, *American Journal of Sociology*, Vol. 93, No. 3, pp. 623–658, ISSN 0002-9602

Shaw, R. B. (1997). *Trust in the Balance: Building Successful Organizations on Results, Integrity, and Concern*, Jossey-Bass, ISBN 978-0-787-90286-5, San Francisco CA, USA

Siegrist, M., Earle, T. C. & Gutscher, H. (Eds.). (2007). *Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind*, Earthscan, ISBN 978-1-84971-106-7, London, UK

Sileo, J. (2010). *Privacy Means Profit: Prevent Identity Theft and Secure You and Your Bottom Line*, John Wiley & Sons, ISBN 978-0-470-58389-0, Hoboken NJ, USA

Six, F. (2005). *The Trouble with Trust: The Dynamics of Interpersonal Trust Building*, Edward Elgar Publishing Limited, ISBN 1-84542-290-2, Cheltenham, UK

Smith, S. W. (2005). *Trusted Computing Platforms: Design And Applications*, Springer Science + Business Media, Inc, ISBN 0-387-23916-2, Boston, USA

Sobh, T., Eleithy, K., Mahmood, A. (Eds.). (2010). *Novel Algorithms and Techniques in Telecommunications, Networking*, Springer Science+Business Media, ISBN 978-90-481-3661-2, Heidelberg, Germany

Sorensen, S. (2010). *The Sustainable Network: The Accidental Answer for a Troubled Planet*, O'Reilly Media, ISBN 978-0-596-15703-6, Sebastopol CA, USA

Thuraisingham, B. (2011). *Secure Semantic Service-Oriented Systems*, Auerbach Publications, ISBN 978-1-4200-7332-4, Boca Raton FL, USA

Tiller, J. S. (2011). *Adaptive Security Management Architecture*, Auerbach Publications, ISBN 978-0-8493-7052-6, Boca Raton FL, USA

Tipton, H. F., Krause, M. (2008). *Information Security Management Handbook, 6th Edition*, Auerbach Publications, ISBN 1-4200-6708-7, Boca Raton FL, USA

Toninelli, A., Pathak, A., Issarny, V. (2010). *Yarta: A Middleware for Managing Mobile Social Ecosystems*, in *Advances in Grid, Pervasive Computing, Proceedings of 6th International Conference, GPC 2011*, ISBN 978-3-642-20753-2, Oulu, Finland, May 11-13, 2011

Tsai, W., Ghoshal, S. (1998). Social capital, value creation: the role of intrafirm networks, *Academy of Management Journal*, Vol. 41, No. 4, Dec 1998, pp. 464–76, ISSN 0001-4273

Veeningen, M., de Weger, B., Zannone, N. (2010). *Modeling Identity-Related Properties, Their Privacy Strength*, in *Formal Aspects of Security and Trust, Revised selected papers of 7th International Workshop, FAST 2010*, ISBN 978-3-642-19751-2, Pisa, Italy, September 16-17, 2010

Victor, P., Cornelis, C., De Cock, M. (2011). *Trust Networks For Recommender Systems*, Atlantis Press, ISBN 978-94-91216-08-4, Paris, France

Viega, J. (2009). *The Myths of Security: What the Computer Security Industry Doesn't Want You to Know*, O'Reilly Media, ISBN 978-0-596-52302-2, Sebastopol CA, USA

Vladimirov, A., Gavrilenko, K., Michajlowski, A. (2010). *Assessing Information Security: Strategies, Tactics, Logic and Framework*, IT Governance Publishing, ISBN 978-1-84928-036-5, Cambridgeshire, UK

Vukovic, Dragutin, (2011). *In Cloud we Trust*, in *KOM 2011 – Electronic Communications Technologies And Standards in Informatics, Proceedings of 22nd Conference, KOM 2011*, ISSN 1334-4463, Opatija, Croatia, November 2011

Waldo, J., Lin, H., Millett, L. I. (Eds.). (2007). *Engaging Privacy and Information Technology in a Digital Age*, The National Academies Press, ISBN 978-0-309-10392-3, Washington D.C., USA

Wheatley, M. J., Kellner-Rogers, M. (1996). *A Simpler Way*, Berrett-Koehler Publishers, ISBN 978-1-576-75050-6, San Francisco CA, USA

Whitener, E. M., Brodt, S. E., Korsgaard M. A., Werner, J. M. (1998). Managers as initiators of trust: an exchange relationship framework for understanding managerial trustworthy behavior, *Academy of Management Review*, Vol. 23, No. 3, Jul 1998, pp. 513–30, ISSN 0363-7425

Windley, P. J. (2005). *Digital Identity*, O'Reilly Media, ISBN 0-596-00878-3, Sebastopol CA, USA

Winkel, B. J., Deavors, C., Kahn, D. (2005). *The German Enigma Cipher Machine: Beginnings, Success, and Ultimate Failure*, Artech House, ISBN 978-1-580-53996-8, Norwood MA, USA

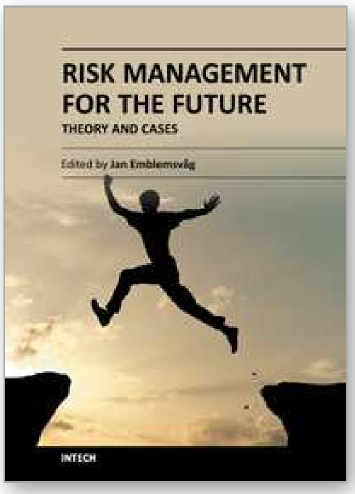
Wong, A., Yeung, A. (2009). *Network Infrastructure Security*, Springer Science+Business Media, ISBN 978-1-4419-0165-1, New York NY, USA

Zagalo, N., Morgado, L., Boa-Ventura, A. (Eds.). (2011). *Virtual Worlds, Metaverse Platforms: New Communication, Identity Paradigms,* Information Science Reference (an imprint of IGI Global). ISBN 978-1-60960-854-5, Hershey PA, USA

Zaheer, A., McEvily, B., Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational, interpersonal trust on performance, *Organization Science*, Vol. 9, No. 2, May 1998, pp. 141–159, ISSN 1047-7039

Zand, D.E. (1997). *The Leadership Triad: Knowledge, Trust, and Power*, Oxford University Press, ISBN 978-0-195-09240-0, New York NY, USA

Zheng, L. et al. (2010). *A Scalable Multiprocessor Architecture for Pervasive Computing*, in *Advances in Grid, Pervasive Computing, Proceedings of 6th International Conference, GPC 2011*, ISBN 978-3-642-20753-2, Oulu, Finland, May 11-13, 2011



Risk Management for the Future - Theory and Cases
Edited by Dr Jan Emblemsvåg

ISBN 978-953-51-0571-8
Hard cover, 496 pages
Publisher InTech
Published online 25, April, 2012
Published in print edition April, 2012

A large part of academic literature, business literature as well as practices in real life are resting on the assumption that uncertainty and risk does not exist. We all know that this is not true, yet, a whole variety of methods, tools and practices are not attuned to the fact that the future is uncertain and that risks are all around us. However, despite risk management entering the agenda some decades ago, it has introduced risks on its own as illustrated by the financial crisis. Here is a book that goes beyond risk management as it is today and tries to discuss what needs to be improved further. The book also offers some cases.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821