WILL THE CLOUD MAKE THE CITIZEN MORE VULNERABLE?

Risk and Vulnerability Assessment in Times of Cloud-computing

Stefan Scheer[1], Ioannis Kounelis[1,2] and Jan Löschner[1]
[1]*European Commission – Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra, Italy*
[2]*Royal Institute of Technology (KTH), Stockholm, Sweden*

Keywords: Digital Citizen, Digital Society, Cloud Computing, Risk, Hazard, Vulnerability, Exposure.

Abstract: Through digital traces that are left behind citizens are more and more exposing their personal data, digital identities to third parties in a conscious or mostly unconscious way. The latter is particularly the case for a variety of cloud computing applications implicitly used by a default citizen. To interact in a digital world and to give away personalized information opens the door for several hazards that may occur – deliberately or not. Consequently a citizen becomes vulnerable in various dimensions. Current research tries to re-apply well-known risk analysis strategies within the new context and in particular to cloud-computing scenarios. Final aim would be to identify individual risks in a qualitative and quantitative manner.

1 INTRODUCTION

In a growing global digital world a citizen is nowadays navigating in various dimensions: advanced use of mobile phones, citizen in motion, being listed in digital archives, putting personalized information on public platforms, etc. While navigating, the citizen is creating a steadily increasing trail of more or less personal data projected and archived in the digital world.

Cloud applications are more and more becoming state-of-the-art from various points of view when it comes to outsource any type of (software-related) service or the externalisation of data repositories. Moreover the externalisation of data is done in a rather hidden way, without explicitly "telling" the user where his/her data are residing. However, externalisation of data transfer and data storage can make a citizen vulnerable as the handing over of rather personal or mission-critical data is similar to handing over your personal belongings to an untrusted person.

Hence a citizen is exposing himself (through his data) and thus making himself vulnerable and putting himself, his personality, his digital assets and commitments at risk.

Obviously, at that point it would be interesting to know up to which extent the classical theory of risk analysis (and even the use of risk analysis tools), mainly applied to vulnerabilities from natural hazards, accidents, etc., could be transferred and re-applied within the context of citizens' digital interactions and in particular to cloud-based applications. In addition, as it seems that many security-related issues are tackled as well, it is the intention of current research to put a focus on the citizen, his vulnerabilities, exposure and ways to handle these problems.

2 CLASSICAL RISK ANALYSIS

Classical risk definitions ((UNDP, 2004) for example) refer to risk as the combination of the probability of an event and its negative consequences. Many refer to a hazard, for the first part, and to vulnerability, describing the second part. Hence, risk is a function of two components 'hazard' and 'vulnerability' whereas the latter frequently is extended towards 'exposure' thus getting the equations (1) and (2) as follows:

$$R = H * V \quad (1)$$

$$R = H * V * E \quad (2)$$

Risk (R) is the magnitude of an interaction of a given hazard (H) with a citizen's vulnerability (V)

Scheer S., Kounelis I. and Loeschner J..
WILL THE CLOUD MAKE THE CITIZEN MORE VULNERABLE? - Risk and Vulnerability Assessment in Times of Cloud-computing.
DOI: 10.5220/0003960801730176
In *Proceedings of the 2nd International Conference on Cloud Computing and Services Science* (CLOSER-2012), pages 173-176
ISBN: 978-989-8565-05-1

and a citizen's exposure (E) towards this. Equation (2) has typically been described by (Crichton, 1999) for the field of risks from natural hazards; Figure 1 shows the dependencies in a graphical way.

Figure 1: The Risk Triangle (Crichton, 1999).

The interpretation of risk means that it is the probability of harmful consequences or expected losses resulting from an exposure to a given hazard.

2.1 Hazard

In the context of a digital world, and in particular while using cloud-computing services, we consider a hazard as signifying a potentially damaging event, phenomenon and/or human activity, which may cause property damage, social or economic disruption. Usually hazards are single events; but we can learn from classical risk analysis that under certain circumstances risks can also be sequential or combined and as such can be summed up (UNDP, 2004). Generally, a hazard is a situation that poses a level of threat; as such a hazard can be dormant or only theoretical. However, within a certain probability a hazard may develop within an incident.

Inherent part of the hazard definition is also the probability that a particular hazard may evolve. In that sense, the occurrence of a specific hazard is out of the scope a citizen is actively navigating in.

The origins or sources for incidents can be manifold: there can be malicious attacks as well as hidden built-in functions on (digital) applications or profiling agents that combine various sources of information in order to derive new data or information (Wright, 2010).

2.2 Vulnerability

Vulnerability which – in the classical definition – is very much related to the general living condi-tions of an individual may – within a wider scope – be extended away from a pure economical condition towards a vulnerability scope affecting more and more the social status of an individual.

With that we mean in particular the affectation of an individual's digital identities, devices and presences on various digital platforms; it can also include (correct) access to information as well as the integrity of an individual's personal data.

Vulnerabilities may arise from situations that can be questioned like: are my data transmitted in a secure way? Are my data which are stored in the cloud available on request? Can my cloud-stored data be restored totally and correctly? Are my cloud-stored data only revealed to me and to nobody else? Do the cloud-based services deliver the right results?

Though not further discussed within the context of this paper, quantifying an individual's vulnerability may also need to take into consideration the individual's own resilience and ability towards applying appropriate mitigation measures thus possibly reducing an individual's vulnerability.

2.3 Citizen Exposure to Cloud Applications

Exposure is the third decisive factor in equation (2); with regard to section '2.2 Vulnerability', an exposure may establish a situation as described in that section. Contrarily to exposure to natural hazards, a citizen's exposure in the cloud is of less physical nature rather than of virtual nature. A citizen may of course exhibit his digital devices to the world, open up unsecured network connections; more exposure, however, may be demonstrated by exhibiting individual information or private data by using digital applications.

Concerning citizens' based cloud-computing the following main types of exposure may be treated:

1. exchange of information and data through network channels;
2. deposit of personal information and data on external devices;
3. request of software services and delivery of results;
4. writing/publishing of personal information/data on (semi-)public internet platforms.

With the availability and the use of several platforms and/or services, a citizen's total exposure will be quantified by summing up every single exposure.

3 CLOUD-DEPENDENT RISKS

3.1 General

Cloud-computing offers a wide range of functionalities and characteristics each of which may be at stake under certain conditions (Jeffery and Neidecker-Lutz, 2010). Often cloud-computing services are used by the citizens without explicitly

knowing about it or explicitly asking for it which means that a default citizen may often not be aware of the under-lying risks.

From a citizen perspective cloud services are often requested for storage and for data/information exchange purposes. Hence PaaS-type cloud services may be prevalent. Moreover cloud services like SaaS may be requested as well, while we assume that from a citizen's perspective the IaaS-use case would be the least requested. In addition, our investigations are focussing on the use of public clouds rather than private ones.

3.2 Availability

Being one of the core aspects of cloud compu-ting, the instant availability of cloud services is essential, simply because each individual strongly relies on the (implicit) promise to get his/her data back. Recent cases have shown that unfortunately this is not always the case (Parnell, 2012a; Parnell, 2012b).

Availability mostly also concerns the instant back-delivery to the user upon request. Cloud-based services, however, operate on the basis of resource-sharing; an instantaneous answer viewable on a user's device may be hampered by too many concurrent requests.

3.3 Reliability and Quality of Service

The reliable delivery and correct restoration of outsourced citizen data is crucial for the acceptance of such services. In that sense the prevention of data losses as well as the restitution of data in its original context is of highest priority. Basically cloud providers are external organisations and as such their functioning may stop without the individual's influence. In the worst scenario the total loss of data may occur (McKendrick, 2011).

Many use cases also require a high quality of service thus reducing response times or increasing the general throughput of data. User vulnerability may vary according to specific user resilience, for example to dispense with a timely restoration of own data.

3.4 Economical and Social Aspects from a User's Perspective

Though business-related economical aspects may play a less critical role for most of the private citizens' use cases, it can nevertheless become an important point in a citizen's portfolio if economical aspects are tackled in an unpleasant way. Users are mostly attracted by free or low-cost services offered through cloud applications. With other words, if this aspect may not be valid any more or if the return-on-investment is too low, a user may easily better refrain from such services rather than continue to pay, at the end, even more than originally planned.

An even more interesting aspect could be derived from an indirect affectation of a citizen's assets (financial, health, reputation, etc.). Obviously, risks to losses or damages of that kind can be tremendous for an individual. Except for the handling of financial losses, the quantification of social damage opens up a new field of investigation.

Citizens as private persons may have little mitigation strategies compared with commercial companies and are often at the mercy of the particular situation; in addition, a wide-spread non-awareness of such risks among the population as well as lack of relevant knowledge makes it more and more important for a citizen to assess his/her individual situation and vulnerability, respectively.

3.5 Psychological Acceptability of Security

Closely related to non-awareness or lack of relevant knowledge is the known fact that individuals tend to underestimate the potential hazard while exposing themselves too much. More-over general observations reveal a contradictory be-haviour towards increased security measures: the installation of relevant measures does not always demonstrate the intended results. Users tend to feel uncomfortable with such measures (Bishop, 2003). Risks deriving from these considerations will have to be addressed as well.

3.6 Ease of Use of Cloud Services and Risks of Negligence

For the individual most of the (hidden) cloud-computing applications are easy to use; in addition, several types of (competing) applications attract the user. Consequently individuals tend to spread their data (in parallel) on various platforms or with several services. The spreading of (same or similar) data on more platforms, however, contributes to an increase of exposure and thus to an increase of risk.

In addition, there is the fact that one and the same cloud provider aggregates its services thus mixing and copying a user's data with other applications; for example, all Google owned services bear the risk that a user's data (and setting) that originally had been provided for one service, may become "available" for other services, too. Hence an increase in a user's exposure is observed.

Connected with a user's easy-to-use attitude is a general negligence (or sometimes impossibility) to wipe out personal information or data. In most cases the original data pertain "for ever", and mostly also without the explicit consent or knowledge of the owner of the data. Recent observations from Social Media sites have revealed that deletion of user data does not entirely mean deletion from the server.

3.7 Security and Privacy Concerns

The full range of security and privacy issues apply for most of the cloud applications, mostly arising from multi-tenancy and concurrency issues. Data in the cloud are shared between multiple tenants. The same resources, e.g. a database, may be (unknowingly) shared among several users. It is obvious that risks regarding security and privacy concerns will arise (Jeffery and Neidecker-Lutz, 2010). What if we envisage a software failure during data restoration (from a commonly shared) database?

Moreover the location of data is potentially not known. For legal purposes it could be extremely difficult to identify a country-specific legal basis in case of a dispute.

3.8 Exploitation of Data

Known business models of cloud-service providers or cloud-computing applications revealed the massive use of information and data provided by individuals for the purpose of commercialisation. Multi-facetted user-provided data can be re-shuffled or aggregated in many different ways thus creating assets of interesting commercial value.

Data are "handed over" to external stakeholders who, in principle, can read, copy, and exploit them commercially. Though data protection principles would usually apply within cloud computing contracts, there is little control over potential exploitation of citizen-own data. Modern social media platform even are deliberately exhibiting user data to more or less defined online communities.

Risks deriving from this way of exploiting user data are of a new dimension and will have to be thoroughly assessed and discussed with ongoing research.

4 DISCUSSION

The aim of the current research is to look into the qualitative and quantitative dimensions of citi-zens' vulnerabilities while interacting in the digital world, and in particular to cloud-computing appli-cations. Therefore, this position paper investigates on the application of classical risk analysis concepts to the particular field of citizen's digital interaction.

Research will define what the single constituents of the classical risk formula (hazard, vulnerability, exposure) mean in the new context; current research should also give hints on how these concepts will be classified and quantified. In a further step the risk formula concept will be applied to a number of common scenarios out of the cloud-computing world which can affect the citizen's assets in general.

Ongoing research will postulate the necessity of detailed classification and subsequent quantification of all risk affecting factors or parameters: incidents for hazard quantification; types of vulnerabilities including individual resilience; types of exposure and possible degrees of exposure.

In a different step, it is planned to apply known risk analysis methods, for example FMEA (Failure Mode and Effects Analysis) or FTA (Fault Tree Analysis); eventually results will be produced that would help to generate a clear statement on the individual risk a citizen takes while navigating in the cloud.

REFERENCES

Crichton, D.: The Risk Triangle, in: J.Ingleton ed., Natural Disaster Management, London: Tudor Rose, pp.102-103 (1999).

United Nations Development Programme (UNDP): Reducing Disaster Risk. A Challenge for Development. A Global Report: UNDP – Bureau for Crisis Prevention and Recovery (BRCP), New York, 2004. Available at: http://www.undp.org/bcpr/disred/rdr.htm .

Wright, D., Safeguards in a World of Ambient Intelligence, Chapter 4: Threats and Vulnerabilities. Springer, 2010.

Jeffery, K., Neidecker-Lutz, B. (eds.): The Future of Cloud Computing, Opportunities for European cloud computing beyond 2010. Expert Group Report, public version 1.0. European Commission, DG Information society and Media, 2010.

Parnell, B.A., Millions face Megaupload data deletion by Thursday, in: <http://www.theregister.co.uk/2012/01/30/megaupload_users_to_lose_data/>, 2012. Accessed 6/3/2012.

Parnell, B.A., Microsoft's Azure cloud down and out for 8 hours, in< http://www.theregister.co.uk/2012/02/29/windows_azure_outage/>, 2012. Accessed 6/3/2012.

McKendrick, J.: Eight cloud computing risks, and how to quash them, in: <http://www.zdnet.com/blog/service-oriented/eight-cloud-computing-risks-and-how-to-quash-them/7752>, 2011. Accessed 5/3/2012.

Bishop, Matt, "Computer Security: Art and Science". Boston, MA: Addison-Wesley, 2003, pp. 348-349.