Visualizing Social, Cloud and Mobile Security Issues

Hamid Nach

Université de Québec à Rimouski,
Campus de Lévis, QC, Canada
hamid_nach@uqar.ca

Abstract: This paper presents a visualization map, in the form of radial Reingold Tilford trees, that depicts the security issues and challenges inherent to SoCloMo – Social, Mobile, and cloud-computing – We used the Data-Driven Documents (D3) JavaScript library to develop the map. The visualization provides a comprehensive overview of the SoCloMo security challenges and their associated mitigation measures.

Keywords: Information visualization, IS security, Social, Cloud, Mobile.

1. Introduction

SoCloMo is the evolution of three key technology trends – social, cloud and mobile technologies – On their own, these technologies are innovative and disruptive; their convergence is having even a greater impact on organizations and industries. SoCloMo creates new business models and makes new venues for customer engagement. However, as with all information technologies, organizations must understand the security threats associated with SoCloMo. Today’s leaders must be very careful to understand the security risks and challenges posed in utilizing these platforms [1]. This paper takes this very perspective. It aims to present an overview of the key security issues encountered when using social, cloud and mobile computing. We display these risks and their associated mitigation measures as a visualization map that we developed for this purpose. Visualizations have the advantage to provide clear and concise view of the domain under study. They also enhance human information comprehension and decision making.

This paper is organized as follows. First, we outline the key security challenges of SoCloMo technologies. After that, we provide a succinct overview of the information visualization field and we describe the process of making the visual map. Finally, we provide a description of the map and we end with a conclusion.

2. SoCloMo security issues

In this section we briefly present key security issues associated with social, cloud and mobile computing.

2.1 Social media

Social media can offer considerable business advantages and benefits to organizations. They entail, however, important security risks [2]. They may be used by hackers as tools to lure their victims as it the case for *dumpster diving* and *social engineering.* Users’ identities can be manipulated to gain access to corporate information. Social media also entails malware which can endanger organization's assets. Examples of such rogue programs are social networking worms, malicious shortened urls, rogue third party apps, and fake plugins.

In order to mitigate these security risks and reap the benefits of social media, companies should first and foremost develop and policy a social media policy [2]. Managers should also reinforce security and privacy awareness among users. Safe-browsing and clicking practices can also help to limit social media risks. Further, deploying identity protection packages is likely to prevent identity usurpation threats.

2.2 Cloud computing

In the recent years, cloud technology is revolutionizing how organizations are doing business. *Cloud computing* enables an on-demand network access to a shared pool of computing resources that can be rapidly provisioned and released [3]. Although cloud computing is offering considerable potential benefits in today's economic environment, it is associated however, with numerous security challenges that should be taken into account. Some of these issues have played a significant role in hindering cloud computing acceptance among organizations [1].

Before decision-makers head to the cloud, they must address profound and legitimate security concerns and systematically address each of them. Many cloud security issues are associated with the data itself, such as unauthorized access, insecure data transfer, data ownership, data leakage, data integrity and data incomplete deletion [4]. Other threats may arise because of shared virtualization and shared IT resources such as side channel attacks, session hijacking, DoS attacks, Botnets network attacks and man-in-the middle [5]. Physical threats are essentially related to outage and disaster [6].

To remediate these problems, managers should adopt a cloud computing security framework that tackles best practices for secure cloud computing operations [7]. The key mitigation measures that have been documented in the IS security literature include, asset protection, network traffic analysis, access and authentication control, data encryption and backups. Companies should also ensure regulatory compliance and deploy a privacy and security policy as well as a business continuity and recovery plan [6, 8].

2.3 Mobile

Mobile technologies have recently grown at a rapid pace, leading to ubiquitous sharing, collaboration and real time access to information [9]. Even though there are several advantages with mobile technologies, they can present serious security risks for organizations. In the last few years, the security of mobile devices has become a top concern for many IT executives, particularly those who pursue a BYOD policy (Bring Your Own Device). Data loss, data leakage, identity theft, mobile data tracking, configuration manipulation, certificate theft are instances of risks associated with mobile computing. These risks stem from a threat which can generally be classified in six categories: 1) malicious apps (e.g. Modular, ransomeware, spyware, phishing), 2) browser-based malware (e.g. malvertizing, framing, browser parasites, cross site scripting), 3) proximity-based hacking (e.g. bluejacking, NFC hacking), 4) OS-based vulnerabilities (e.g. backdoors, keyloggers, sideloading, trojans and viruses), 5) physical threats such as stolen or lost devices, and finally, 6) network threats (e.g. Wi-Fi Sniffing)

To defend against these threats, managers need to develop an effective strategy for enterprise mobile security that establishes policies and procedures [9]. In this regards, implementing malware protection tools (antitheft tools, anti-virus, anti-spyware, anti-phishing), and apps behavior monitoring is likely to reduce the risks associated with mobile applications [5]. OS regular updates and data encryption can also help mitigate the security risks of mobile computing. Companies can also determine what content and resources can be accessed through mobile devices and which cannot. To reinforce security, all mobile devices should offer remote data deletion and tracking capabilities.

3. Method

As we mentioned above, this work aims to develop a visualization map of the key security issues of SoCloMo and their mitigation risks. Visualization is a way of representing data and information as a visual image [10]. It aims to communicate technical information or knowledge in a graphical and understandable way which can ultimately improve managerial judgment [11].

Information visualization is defined as “a computer-aided process that aims to reveal insights into an abstract phenomenon by transforming abstract data into visual-spatial forms” [12]. Its purpose is to “optimize the use of our perceptual and visual-thinking ability in dealing with phenomena that might not readily lend themselves to visual-spatial representations’ [12]. Information visualization is relatively a new field, but it is presenting itself as a viable discipline as it now benefits from developments in technologies that offer innovative ways of presenting complex data and information [10]. Many experts have created inspiring data visualization [13]. Scientists frequently tell stories using visualizations of scientific data, in the process of disseminating findings to peers and to the public [14].

In this section we briefly describe our approach for developing the map. Five major steps were carried out:

- First, a literature review was conducted to uncover what is known in the body of knowledge related to SoCloMo security issues.
- A second step involved the identification of the main concepts related to the topic. About 220 concepts were identified at this stage, they were merely presented as a list.
- The third step involved organizing this list in a hierarchical structure. This process focused on two types of relationships: Meronymic relations—A is part of B—and hyponymic relations— (A is a B). There are three main approaches to developing a hierarchy of concepts The first is a top-down development process that begins with a definition of the domain’s most general concepts and continues with concept specialization; the second is a bottom-up process that starts by defining the most specific concepts and continues by grouping them in more general concepts; the third is a process combining these two approaches. For this study, we have chosen the combined approach. At the very beginning, the most important concepts are defined, then, they are accordingly generalized or specialized into others concepts. Merging and organizing the concepts brought the total concepts to 165.
- The fourth step consisted of the development of the radial structure using the Bostock’s Data-Driven Documents (D3) JavaScript library[1]. D3. J's is a library that uses digital data to drive the creation and control of dynamic and interactive graphical forms which run in web browsers[2]. The type of graph that is represented is based on the radial Reingold Tilford tree. Mike Bostock’s library is increasingly used and provides a powerful set of dynamic visual methods.
- Finally, the rendered SVG graph was exported to Adobe Illustrator, at this stage, the final layout was created and refined.

4. Results

The visualization map we developed (figure 1) highlights the main security issues encountered in social media, cloud computing and mobile technologies (SoCloMo). It also depicts the key risk mitigation measures as they are presented in the scientific literature. The online version of the map can be found at the following address:

http://goo.gl/0G9Xrm

The visualization is based on the Reingold Tilford tree. The hierarchical structure that we used displays the concepts in a way that expands outwards, radially. First the user is able to

[1] http://d3js.org/

[2] http://en.wikipedia.org/wiki/D3js

have an overview of the entire map to understand the complete structure of the knowledge space. After gaining an overview, the user is able to focus on entities of interest by using the zoom navigation buttons or by mouse movement. The reader can "navigate" the map without losing quality of the images presented. While the security threats and risk concepts present in a hierarchical structure, the mitigation measures are presented a concentric ring [15].

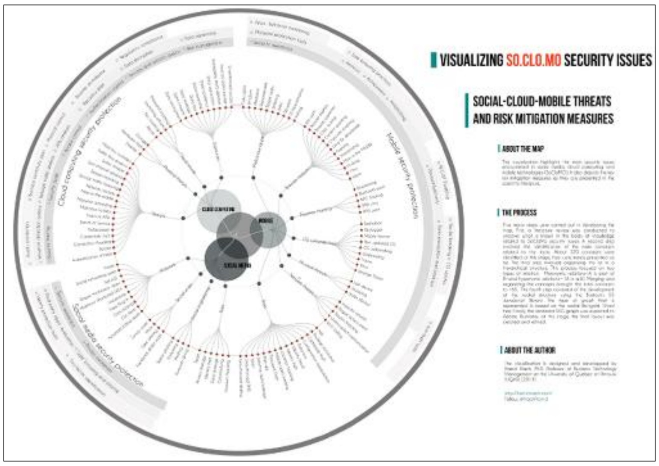
VISUALIZING SO.CLO.MO SECURITY ISSUES
SOCIAL-CLOUD-MOBILE THREATS AND RISK MITIGATION MEASURES
ABOUT THE MAP
THE PROCESS
ABOUT THE AUTHOR
Cloud computing security protection
Mobile security protection
Social media security protection
CLOUD COMPUTING
MOBILE
SOCIAL MEDIA

Figure 1: The map's final layout

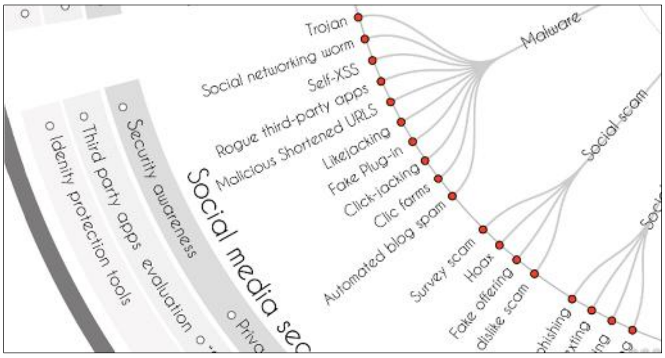

Figure 2: A close-up view on social media security risks

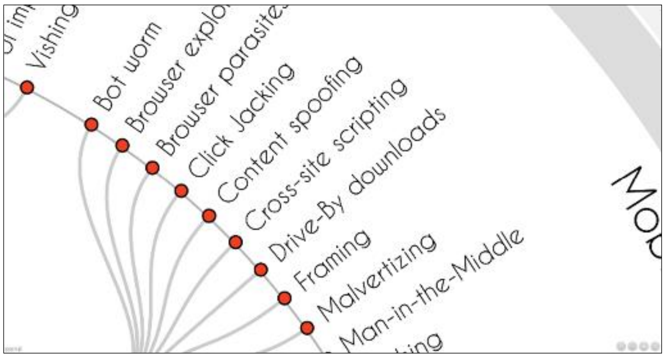

Figure 3: A close-up view on mobile security risks

5. Conclusion

There are many new technologies emerging at a rapid rate, each with the promise of efficacy and efficiency. This is the case of SoCloMo technologies. Despite the potential gains achieved from the social, cloud and mobile computing, there are security issues and challenges that should considered. This works contributes by developing a visual map that offers a comprehensive overview of SoCloMo security issues and their key reponses. The concepts are easily communicated and are presented within an easy reach of the user. The map would ultimately help decision makers better understand the security threats inherent to SoCloMo. It can also be used for education purposes as students can grow aware of the challenges of social, cloud and mobile computing and develop the appropriate skills to tackle them. As a final thought, we hope the work we present in this paper would provide convincing arguments about the information visualization value as an analytic tool. Future research may use information visualization in more innovative ways and develop, for example, interactive maps where users can search and explore information in an intuitive way.

References

[1] S. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud Computing Security Issues and Challenges," *International Journal of Computer Networks,* vol. 3, pp. 245-255, 2011.

[2] M. Chi, "Security Policy and Social Media Use." Reducing the Risks of Social Media to Your Organization," *SANS Institute InfoSec Reading Room,* 2013.

[3] N. Dirk, *Mobile Strategy for Your Company: SoCloDaMo (Social + Cloud + Big Data + Mobile)*: IBM Press, 2013.

[4] Z. Dimitrios and L. Dimitrios, "Addressing cloud computing security issues," *Future Generation Computer Systems,* vol. 28, pp. 583–592, 2012.

[5] A. Cecil Donald, S. Arul Oli, and L. Arockiam, "Mobile Cloud Security Issues and Challenges: A Perspective," *International Journal of Engineering and Innovative Technology* vol. 3, pp. 401-406, 2013.

[6] F. Sabahi, "Cloud computing security threats and responses," 3rd IEEE International *Conference on Communication Software and Networks (ICCSN),* Xi'an, 2011 pp. 245 - 249.

[7] D. Jamil and H. Zaki, "Cloud Computing Security," *International Journal of Engineering Science and Technology,* vol. 3, pp. 3478-3483, 2011.

[8] P. Scott, T. Paul, and C. Susan, "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly,* vol. 27, pp. 245–253, 2010.

[9] Gurpreet et al., "Convergence of Social, Mobile and Cloud: 7 Steps to Ensure Success " Cloud Standards Customer Council 2013.

[10] J. H. Larkin and H. A. Simon, "Why a diagram is (sometimes) worth ten thousand words," *Cognitive Science,* vol. 11, pp. 65-99, 1987.

[11] C. M. Foil and A. S. Huff, "Maps for managers: Where are we?, Where do we go from here?," *Journal of Management Studies,* vol. 29, pp. 267-285, 1992.

[12] C. Chen, "Information visualization," *Information Visualization,* vol. 4, pp. 1-4, 2002.

[13] J. Moody and K. Healy, "Data Visualization in Sociology," *Annual Review of Sociology,* vol. 40, 2014.

[14] M. Kwan-Liu, C. Davis, I. Liao, J. Frazier, and H. Hauser, "Scientific Storytelling Using Visualization," *Computer Graphics and Applications, IEEE,* vol. 32, pp. 12 - 19, 2012.

[15] D. Stephan, B. Fabian, and B. Michael, "Uncovering Strengths and Weaknesses of Radial Visualizations—an Empirical Approach," *IEEE Transactions on Visualization and Computer Graphics,* vol. 16, 2010.

Hamid Nach, Ph.D. is professor of information systems at the University of Quebec at Rimouski, Lévis Campus. Dr. Nach worked in the private sector for about 10 years before he enrolled in academia. He teaches undergraduate and graduate classes in the field of information systems. His research interests concerns generally the study of how people use and transform information and communication technologies (ICT) and how, in return, ICT transform their lives. His teaching covers a wide range of Business-Technology-Management related areas such as, IS strategy, IT management, cloud computing, ecommerce and social media.