Computers in Industry 88 (2017) 1–11

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Web 2.0 applications in the workplace: How to ensure their proper use?

Noura Faci [a], Zakaria Maamar [b,*], Vanilson Burégio [c], Emir Ugljanin [d], Djamal Benslimane [a]

[a] Claude Bernard Lyon 1 University, Lyon, France
[b] Zayed University, Dubai, United Arab Emirates
[c] Federal Rural University of Pernambuco, Recife, Brazil
[d] State University of Novi Pazar, Novi Pazar, Serbia

ARTICLE INFO

Article history:
Received 30 June 2016
Received in revised form 1 January 2017
Accepted 9 March 2017
Available online 28 March 2017

Keywords:
Hangouts™
Restriction
Social action
Web 2.0 application

ABSTRACT

There is an ongoing debate about the role of Web 2.0 applications (e.g., Facebook™ and Instagram™) in the workplace. Indeed, misuse cases of these applications are on the rise and many enterprises still have concerns with their real benefits and values and thus, have been reluctant to adopting them. This paper addresses these concerns by developing restrictions over the social actions that Web 2.0 applications allow users to perform. These restrictions permit to limit for instance, the number of times a social action is performed, the content of a social action, and the recipient of a social action. The restrictions are specified in UML Object Constraint Language and enforced through a run-time monitoring that permits to detect violations. This paper, also, presents an implementation of restrictions over Hangouts™ as an illustrative Web 2.0 application.

1. Introduction

Despite the excitement about Web 2.0 applications and technologies, many enterprises still question their appropriateness for the workplace. In this section, we discuss the motivations that justify organizations' concerns along with an illustrative case-study.

1.1. Motivations

There is a continuous "pressure" on today's enterprises to be creative and innovative, so they can tackle multiple challenges such as political, economical, and societal. Enterprises are embracing Information and Communication Technologies (ICTs) to ensure competitiveness, responsiveness, and effectiveness despite all these challenges that could slow down their growth and put their survival at risk, for example. The World Wide Web (Web for short) illustrates perfectly the ICT support to enterprises that would like to have an efficient online presence on the Internet. Although the R&D community has been examining the Web from a technical perspective [11,18], a social perspective has emerged lately as a direct result of the rapid advances of Web 2.0 technologies. According to Global Industry Analysts, Inc. "*The global expenditure on Enterprise Web 2.0 is forecast to reach $5.7 billion by 2015, driven by expanding broadband capabilities, decreasing prices, improving performance of networks, and the development of advanced, highly interactive Web 2.0 applications*" [24] and "*. . .the top 15 Web 2.0 vendors will spend $50 billion in 2015 on servers, networks, and other infrastructure, up from $38 billion in 2014 and $30 billion in 2013*" [23].

Despite all the excitement (and sometimes "hype") about Web 2.0 technologies and applications, many enterprises still have concerns with their real benefits and values and thus, have shown some resistance in adopting them [7]. According to Gartner, "*. . .many large companies are embracing internal social networks, but for the most part, they're not getting much from them*" [10]. Enterprises see a limited return-on-investment of these technologies in their operations and see them mainly as a source of distraction to employees and also a source of security breaches (the average cost of a data breach for an enterprise rose from $6.65 million in 2008 to $6.75 million in 2009 [21]). Misuse cases of Web 2.0 applications (e.g., Facebook™ and Twitter™) are increasing at an alarming rate and the serious lack of guidelines and awareness is widely used to justify these cases, i.e., "nobody told me" is a valid excuse. Investigating security threats of Web 2.0 applications is, also, important but this does not fall into the scope of this paper.

In [14], we present our recommendations to enterprises on how to address concerns with Web 2.0 applications by developing restrictions over social actions. These restrictions would "explain"

* Corresponding author.
E-mail address: zakaria.maamar@zu.ac.ae (Z. Maamar).

http://dx.doi.org/10.1016/j.compind.2017.03.003
0166-3615/

what to do (e.g., posting notes is allowed but engaging in chat sessions is not) and how (e.g., poke should be used), when (e.g., only during peak-off hours), and where (e.g., only in the office) to do it. Our restrictions permit to limit for instance, the number of times a social action is executed, the content of a social action, and the recipient of a social action. In [14], our contributions include a list of social actions that some representative Web 2.0 applications allow users to execute; a specification of restrictions over social actions using a language for instance, UML Object Constraint Language (OCL); and a monitoring approach to detect restriction violations so that compliance with restrictions is guaranteed. In this paper, additional contributions include a discussion on how enterprises embrace Web 2.0 applications so they become social enterprises (*aka* enterprise 2.0); and a complete social-action restriction system for Hangouts™ as an illustrative Web 2.0 application.

1.2. Case study

Our case study is about a travel company that has grown considerably in a short period of time. The company consists of different departments including `call centre` that books and issues tickets; `cargo & logistics` that handles freights and develops tailor-made shipping solutions; and `professional development` that runs training for employees and partners.

The company's growth is somehow due to its aggressive marketing through social media such as regular posts on Twitter™ and updates of Facebook™ pages. Despite the strong presence in social media, the main online communication means with stakeholders remains emails and/or online forms. Recently, some stakeholders suggested that live conversations with certain of the company's departments would expedite the processing of their requests. Indeed, a chat tool like Hangouts™ would support real-time conversations through the following examples:

1. Respond to customers' online requests. Travel consultants would initiate live chat sessions with customers to answer their questions in real-time.
2. Organize meetings. Staff from different departments would hold meetings on collaborative projects.
3. Conduct Webinars. Training would be streamed without having to worry about trainees' locations and time zones.

Despite the positive uses of Hangouts™, it has become a source of concerns for the company's senior management due to lack of guidelines associated with how, when, and where to use it. Several misuse cases have been identified like excessive chat hours, inadvertent online disclosure of sensitive content, and overuse of multimedia material. More details on each case are provided below.

- Excessive chat hours: supervisors should investigate the excessive durations of certain chat sessions; this could reveal the inefficiency of some travel consultants and/or complexity of some customers' requests, for example. Excessiveness undermines the company's five-minute promise to respond promptly to customers' chat requests.
- Inadvertent online disclosure of sensitive content: prior approval of what can be posted online could be violated if not communicated properly nor enforced at run-time. Disclosures involve marketing plans that could undermine the company's competitive advantage.
- Overuse of multimedia material: although some departments (e.g., professional development) depend heavily on multimedia, their overuse could slow down the company's network during peak-hours.

Challenges like how to "keep an eye" on what is happening, how to ensure that only specific employees make video calls, and how to gear chat sessions towards customers, only, will surface all the time if not tackled properly. We aim at assisting enterprises adjust their use of Web 2.0 applications based on factors like types of stakeholders (returning customers *versus* new customers), sensitivity of content (marketing plans *versus* financial statements), and types of Web 2.0 applications (Facebook™ *versus* Hangouts™).

1.3. Paper organization

The remainder of this paper is organized as follows. Section 2 is an overview of some misuse cases that undermine Web 2.0 applications' success along with a definition and architectural representation of the social enterprise. Section 3 discusses our approach in terms of defining properties of social actions, defining restrictions, enforcing restrictions over social actions, and finally demonstrating this enforcement through a system. Section 4 is about future and finally, Section 5 concludes the paper.

2. Background

This section discusses Web 2.0 applications misuse from a security and privacy perspective. Unfortunately this misuse is addressed with corrective and not preventive actions. This is somehow late due to these cases' serious impacts on people's personal lives. The section also presents how enterprises become social from an architectural perspective.

2.1. Web 2.0 applications misuse

There is an ongoing (sometimes "heated") debate about the role of Web 2.0 applications in today's life, in general, and the workplace, in particular. On the one hand, pros include reaching out to more people and tapping into social data. On the other hand, cons include distracting employees and facilitating security breaches [21]. On top of securing Web gateways to address these breaches, we deem important "controlling" the actions that could lead into breaches. In the R&D community (e.g., [2,3,6,19,13,22]), the focus is still on dealing with the security and privacy of data of Web 2.0 applications. Approaches that educate users on how to use Web 2.0 applications efficiently and/or suggest preventive instead of corrective actions, are still limited. To the best of our knowledge, there is a serious lack of such approaches. Cases like circulating photos on the Web and posting personal information show the severe damages that these actions have on people's personal lives [20]. Wouldn't it be better to "control" the actions of circulating and posting before performing them?

Bhatti et al. [3] conduct an empirical evaluation of the role of access controls in enterprises that use social-media applications. The authors associate controls with federal and state regulations that define how data employees can be accessed and shared through these applications. For instance, "*. . .any inadvertent release of this data to unintended recipients will result in a significant privacy breach, and hence access controls must be in place to ensure that messages are always sent securely by authorized users*" [3]. Unfortunately, Bhatti et al.'s access control does not consider the social actions that employees execute in terms of frequency, time, validity, etc. These actions' outcomes are potential sources of data breaches.

Dinerman [6] discusses security risks in the context of social networking and mentions that nobody can question the benefits of Web 2.0 applications like Facebook™, Twitter™, and LinkedIn™. In addition to this usefulness, these applications come with their own set of security concerns that can put data integrity and confidentiality at risk. Dinerman stresses out that tweets like