Online Social Media Networking and Assessing Its Security Risks

Hak J. Kim

Hofstra University
hak.j.kim@hofstra.edu

Abstract

Over the past several years, we have seen the emergence of new paradigm in the Internet, online social media networking, which provide Internet users to communicate and collaborate with family, friends, social groups, and other community by using social media tools (i.e., Twitter, Facebook, MySpace, and Youtube). The use of social media for communication is becoming more prevalent worldwide, with people from countries of varying economic development increasingly accessing the Internet to participate in networking sites. Online social media networking today is a great tool to meet and network with people sharing similar business interests. However, they can also pose serious security threats to users and their organizations. This paper presents the security risks of online social media networking and then attempts to develop the model for assessing its security risks. Our model can help security professionals for assessing security risks in the existing information systems and designing new security systems of enterprise.

Keywords: *Online Social Media, Social Networking, Security Risks, Trust Zone*

1. Introduction

Today online social networking applications [1] are rapidly growing in use both personally and professionally. The use of social networking is becoming more prevalent worldwide, with people from countries of varying economic development increasingly accessing the Internet to participate in networking sites. With the popularity of mobile devices and applications combined with social networking technologies, communication using online social networking tools is becoming a new way of life to the people [2]. Facebook [3] is one of the strongest growth social networking services and currently more than 500 million users enjoy it for games or sharing information in web applications. Actually social networking is not new. Like traditional social networking in club for party and seminar, online social networking is to communicate between people with similar interests in the Internet [4, 5, 6].

Since most people access social network sites from the comfort and privacy of their home or office, they can be lulled into a false sense of anonymity. Additionally, the lack of physical contact on social network site can lower users' natural defenses, leading individuals into disclosing information they would never think of revealing to a person they just met on a street.

Modern enterprises are heavily relying on information systems; for example, timesharing systems over mainframe computers in 1960s and 1970s, networked personal computers and workstations in 1980s, and Internet-based systems in 1990s [7]. But especially over the past several years, we have seen the emergence of new paradigm in communication systems, called ‘online social networking’, ranging from MySpace to Facebook, LinkedIn, and Twitter. New enterprise environments, communications with social networking platforms, are emerged [8]. That is, social media and online social networking applications are changing the enterprise environment. More than 40% of IBM employees work regularly from customer locations and home rather than on IBM premises [2]. Similarly, Cisco [8] reported ‘more than 60 percent of employees believe that being in the office is no longer needed to be productive’. Sturdevant [9] shows that social collaboration tools are poised to increase productivity. Gupta & Carpenter [10] points out that enterprise value is heavily dependent on employees’ knowledge and their ability to share that knowledge. They also emphasize active employees in social networking for increasing enterprise value. Thus, the enterprise value depends on multiple factors beyond simple activity metrics.

Companies often use online social networks for recruitment and publicity campaigns. Consequently, many companies allow employees to access online social networking sites. However, it might not be such a good idea from the perspective of network security. There have been cases of Facebook and MySpace accounts being hijacked and user names and passwords being sold to underground networks. Hackers then use the compromised accounts to run phishing scams. Safeguarding the network from the vulnerabilities prevalent in social networks is a new and growing challenge in the field of cyber security.

Then, why do enterprises struggle with social media and online social networking applications? Because they are not just the tools, but how their employees use these tools in the working place. Enterprises are trying to make the most of the advantages of online social networking and keep their employees happy, while at the same time, limiting the dangers posed by the increased exposure of potentially sensitive and exploitable information. Since online social networking by company employees continues to be a security concern, enterprises are prompted to look at the risks of them associated with employees’ use and examine the information posted on social networking sites [11].

This paper discusses security risks of SNS at the enterprise and then assesses SNS systems risks using the analytic hierarchy process (AHP) approach which is a useful tool to assist decision makers in reducing complexity to solve problems.

2. Social Media Networking

As traditional social networking (i.e., club, party, seminar, etc.) communicates between people with similar interests in physical spaces, online social media networking is the same with it except for the place to meet; from physical space to cyberspace, especially the Internet [5]. One of the strongest growth areas has been in the adoption of social networking sites, such as Facebook [3] and currently more than 500 million users in Facebook enjoy games or sharing information in web applications. With the popularity of mobile devices and applications combined with social networking technologies, communication using online social networking tools is becoming a new way of life to the people [2].

Online social network services, such as Youtube, MySpace, Facebook, LinkedIn, and Twitter. involving individual Internet users as well as multiple organizations are emerged as new communication platform in today’s dynamic and complicated Internet-based business world. However, with the explosive growth of social media coupled with applications, securing user’s information and the related systems is extremely challenging. Figure 1 shows the generic network architecture for online social network services.

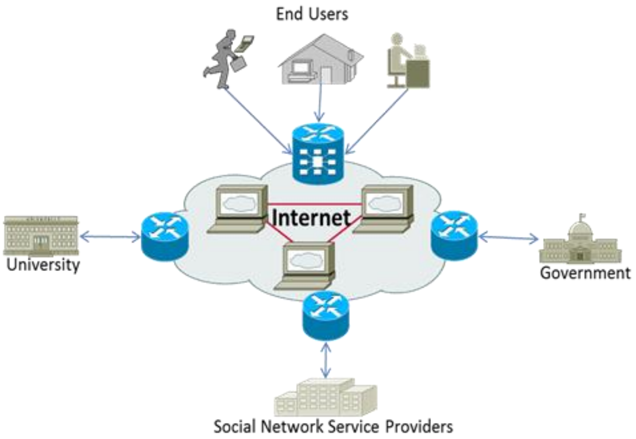

Figure 1. Social Media Network Architecture

Figure 2 show the service framework of SNS. It consists of three parts; user applications, social media devices, and network infrastructure. User applications include web services, e-mail services, instant messaging services, and other services. Current available devices are mobile phones (i.e., iPhone), tablet PC (i.e., iPad), laptop computers, and desktop computers. Network infrastructure includes traditional LAN/WAN, mobile-based wireless networks, and cable networks.

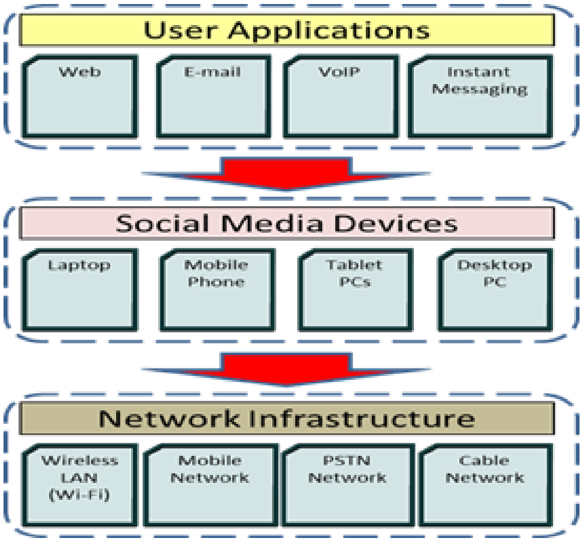

Figure 2. Hierarchy of Social Media System

Social media can be used in e-business, for example user ratings and reviews, user recommendations and referrals, social shopping (sharing the act of online shopping together), user forums and communities, social media optimization (for e-commerce), and social applications and social ads linked to e-commerce. It also can be used in a firm's business functions, as shown in Table 1.

Table 1. Social Media Business Platform

Business	Social Media
Customer Relationship	• Listen to customer concerns • Solve problems • Spread best practices
Human Resource	• Promote company among potential employees • Identify/gather information on job candidates
Production	• Solicit ideas, opinions, and feedback to incorporate them into existing and/or new products and services
Service Delivery	• Enhance collaboration on projects and service engagements • Create and share knowledge • Collaborate on documentation

3. Security Risks and Trust Zones

3.1. Security Risks

Today, many people provide judgment in ensuring trust of social networking while in the Internet; any one or even multiple sets of data can have flaws and impreciseness and still meet the mission of reliable communication. The typical examples of SNS's security risks include account compromise (i.e., e-mail by social media), monetary fraud (i.e., a payment platform in devices), and so on.

However, the total loss or unavailability of some data can be detrimental to ensuring the trust of social media use. As an example, if personal data (i.e., name, photos, address, schools, etc.) and/or related party communications are rendered altogether unavailable to an SNS providers, there is one less human providing judgment; the controller is one of the most important roles in terms of safe travel in addition to the pilot. Therefore, availability is the most important aspect of security relative to confidentiality and integrity to enable the mission. The next priority is integrity, then confidentiality.

Figure 3 shows trust zones are formed around online social media networking systems functions; security boundaries represent all feeds into and out of zones. Each of the three trust zones has very different goals in terms of cyber security and defending against attacks.

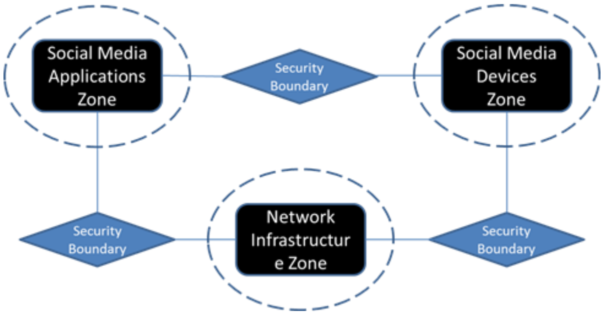
Social Media Applications Zone
Security Boundary
Social Media Devices Zone
Security Boundary
Network Infrastructur e Zone
Security Boundary

Figure 3. Security Trust Zones for Social Media Networking

3.2. Security Trust Zones

The *Social Applications Trust Zone* is comprised of the social network service (SNS) membership registration, SNS applications installation, and SNS processing. Threats in this trust zone include registering criminals obtaining credit card and other personal information for identify fraud and other criminal activities. As a result, encryption, strong identification and authentication, and role based access are incredibly important financial transaction and personal identity activities such as the registering member's identity verification.

The *Social Media Device Trust Zone* will have strong elements of all three aspects of security: confidentiality, integrity, and availability. This trust zone must focus on ensuring that authorized users only have access to devices necessary to perform security functions. Threats include unauthorized users viewing and modifying data, including the insider, and denial of service so authorized users and applications cannot be processed rapidly.

Whereas the social media device trust zone ensures all three principles are fully addressed, the *Network Infrastructure Trust Zone* is focused primarily on ensuring communications and data are available at all times.

4. Assessing Security Risks

For assessing SNS's security risks, the analytic hierarchy process (AHP) approach is introduced. AHP is a useful tool to assist decision makers in reducing complexity to solve problems. We attempt to assess security risks based on each trust zone as addressed in the above.

4.1. Analytic Hierarchy Process (AHP) Approach

AHP was developed in the 1970's by Thomas Saaty [12]. It has grown steadily over the last 40 years, and can be applied to many different applications. In information systems security, AHP studies [13, 14, 15] have included guiding information security investment decisions, evaluating antivirus and content filtering products, and using analytic models on security systems. Saaty [12] proposed a process to break down complexity into smaller scope comparisons, assign relative ratings, and analyze the results to determine the best outcome. His method consisted of defining the problem, or what is to be solved; determining the structure using a decision hierarchy, which includes determining the criteria and alternatives; comparing the alternatives and criteria in pairs to determine preferences and priorities; and analyzing the resulting priorities and preferences to determine the best outcome or alternative to choose to solve the problem. Using this process, AHP can assist decision makers and security professionals in group decision making to address a complex problem.

4.2. Applying AHP to SNS

The first set to determine the optimum security controls for the SNS trust zone. It considers the mission of the SNS, which is to continue to ensure trust communication. Next, the criteria are established identifying the specific threats and vulnerabilities imperative to be addressed by the alternatives. In applying cyber security risk assessment principles, a threat and vulnerability must be coupled to create a resulting impact. That is, a specific threat must exploit, or otherwise exercise, a vulnerability for a successful attack to occur. The criteria (Table 2) are then listed in terms of confidentiality, integrity, and availability for simplifying evaluation.

Table 2. Criteria Assessment

Confidentiality (Rating: 1)	• Intercepted data through unauthorized access (1)
Integrity (Rating: 2)	• Damage to data through Modification of system (3) • False readings due to data corruption (3) • Unpredictable results due to software bugs (miscalculations) (2) • Damage through unauthorized access (3)
Availability (Rating: 3)	• Loss of communications (3) • System damage or crash (denial of service) (3) • Disruption of service (3)

Finally, the alternatives are established. The alternatives (TABLE 3) are all the possible countermeasures or administrative, logical (or technical) or physical security controls to be considered. The chosen controls are derived from National Institute of Standards and Technology (NIST) Special Publication standard 800-53 [18].

Table 3. Alternatives Assessment

Confidentiality (Rating: 1)	• Encryption in transit (1) • Encryption at rest (1) • Access controls (1) • identification and authentication to ensure confidentiality (1)
Integrity (Rating: 2)	• Check hash values of software, applications, scripts (6) • Digital signatures • Software testing and validation (2) • Timestamps (4) • Configuration management (6) • Access controls to ensure identity authentication (6)
Availability (Rating: 3)	• Redundant communications network lines (9) • Spread spectrum (9) • Multiple sources of data provided (9) • High availability servers on certain data sources (9) • Contingency planning (9)

In considering the complexity of ensuring the SNS mission, all three types of controls must be employed. The sample list is not exhaustive, but rather highlights the more salient controls or classes of controls to be considered. To conduct a full and complete risk assessment, all of the baselines controls referred to in Appendix D of NIST Special Publication 800-53 might be considered. The security controls are identified terms of the criteria. Each control will address a specific cyber threat/vulnerability vector (as described in terms of impact).

5. Managerial Implication

In comparing of availability, confidentiality, and integrity, the nature of SNS data is important. Much of SNS data has a short time to live. Once data have sent, the value of keeping the data confidential is minimal in terms of security attacks. Compared to integrity, availability is more important to available data than trust data. So, in our paper, availability is the most important aspect of security relative to confidentiality and integrity to enable the service. The next priority is integrity, then confidentiality. The ratings reflect the priority, with 1 the lowest, and 3 the highest priority.

The SNS trust zone risk assessment is the first step of analyzing and determining the security controls of an international airport information systems infrastructure. A similar risk assessment approach is necessary to apply to the other two trust zones as well for completeness. The social media trust zone would be considered in terms of confidentiality to address the financial and personal data involved. Encryption of financial data will weigh into ensuring the confidentiality of this data. The network infrastructure trust zone may be considered in terms of all three security principles, and might require the highest degree of controls to ensure the security of the information systems in Security trust zone. In addition to strong security boundaries with tight firewall rules, monitoring of security personnel and limiting physical access, where possible, will also be important.

In applying risk assessment using AHP principles, decision makers might consider the method has impreciseness built in. Preferences to certain controls may consciously or unconsciously bias the results in exercising the methodology. In addition, decision makers might have intentional or unintentional motivating factors such as self-preservation from unwanted politics and this may be reflected in not choosing unpopular security controls. Another consideration in applying the methodology is security controls or countermeasures can either partially or entirely address threats and vulnerabilities, and may be interdependent. Choosing the impacts to encompass classes of threats and vulnerabilities may assist in minimizing the interdependency. A final consideration in applying this methodology is the cost of the controls. Risk assessment considers cost as a factor in mitigating the impact of a threat-vulnerability pair. If the cost exceeds the willingness to take the risk, the countermeasure or control is not worth the cost to employ. Similarly, in the example the controls mentioned must be considered with the risk. Redundancy of communication lines can be extremely expensive. However, when the risk is losing lives if the communications lines go down, the cost is most likely worthwhile. Assessing the controls in terms of cost and value are also important in employing the methodology.

6. Concluding Remarks

The SNS systems are a complex multi layered informational system supporting security, operations, vendors, and travelers. They require high levels of computational power in a secure environment. Risk management of information can be mitigated with a good information security management system. The future of SNSs is going to need for more access for users as technology advances and SNS use new techniques.

In summary, applying security risk assessment using the AHP methodology can provide the security professional with a solid approach to complex design of security controls. In SNS systems operations, complexity of diverse business lines coupled with tight regulation add dimensions of complexity that are extremely challenging to any decision maker. Breaking the diverse operations into trust zones and approaching each trust zone with unique criteria and alternatives can tailor security controls. Each trust zone will have threats and vulnerabilities that are specific to the missions and functions, and will vary in impact importance from trust zone to trust zone. The analysis of alternatives will assist decision makers in establishing effective security controls.

References

[1] B. J. Jansen, M. Zhang, K. Sobel and A. Chowdury, “Twitter power-tweets as electronic word-of-mouth”, Journal of the American Society for Information Science andTechnology, vol. 60, no. 11, **(2009)**, pp. 2169-2188.

[2] S. Hathi, “How Social Networking Increases Collaboration at IBM”, Strategic Communication Management, vol. 14, no. 1, **(2009)**, pp. 32-35.

[3] M. K. Foster, A. Francescucci and B. C. West, “Why Users Participate in Online Social Networks”, International Journal of e-Business Management, vol. 4, no. 1, **(2010)**, pp. 3-19.

[4] M. Bulearca and S. Bulearca, “Twitter: a Viable Marketing Tool for SMEs?”, Global Business & Management Research, vol. 2, no. 4, **(2010)**, pp. 296-309.

[5] M. Häsel, “OpenSocial: An Enabler for Social Applications on the Web”, communications of the ACM, vol. 54, no. 1, **(2011)**, pp. 139-144.

[6] K. J. Lacho and C. Marinello, “How Small Business Owners Can Use Social Networking to Promote Their Business”, Entrepreneurial Executive, vol. 15, **(2010)**, pp. 127-133.

[7] M. A. Cusumano, “Technology Strategy and Management: Platform Wars Come to Social Media”, Communications of the ACM, vol. 54, no. 4, **(2011)**, pp. 31-33.

[8] Cisco, Social Media: Cultivate Collaboration and Innovation, white paper, Cisco Inc., **(2010)**.

[9] C. Sturdevant, “Socializing the Enterprise”, eWeek, vol. 28, no. 1, **(2011)**, pp. 34-34.

[10] P. Gupta and H. Carpenter, “Enterprise wide Social Networking Business Intelligence”, Siliconindia, vol. 12, no. 3, **(2009)**, pp. 26-29.

[11] M. Beckman, “Enterprise Security vs. Social Media”, System iNEWS, **(2010)** September, pp. 21-27.

[12] T. Saaty, “Decision making with the analytic hierarchy process”, International Journal of Services Sciences, vol. 1, no. 1, **(2008)**, pp. 83-98.

[13] M. Farrokh, “Evaluation and selection of an antivirus and content filtering software”, Information Management & Computer Security, vol. 10, no. 1, **(2002)**, pp. 28-32.

[14] L. Bodin, L. Gordon and M. Loeb, “Evaluating information security investments using the analytic hierarchy process”, Communications of the ACM, vol. 48, no. 2, **(2005)**, pp. 79-83.

[15] S. Kim and H. Lee, “A study on decision consolidation methods using analytic models for security systems”, Computers & Security, vol. 26, no. 2, **(2007)**, pp. 145-153.

[16] T. Scholtz, “The structure and content of information security architecture”, Report, **(2008)**.

[17] J. Wright and J. Harmening, “Security Management Systems: Security Controls”, In Vacca, J. (Ed.), Computer and Information Security Handbook **(2009),** Boston, MA: Morgan Kaufmann Publishers.

[18] NIST, Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53. Rev.3, Appendix D, Gaithersburg, MD: National Institute of Standards and Technology, **(2009)**.

Authors

Hak J. Kim

He is an associate professor of the Department of Information Technology and Quantitative Methods (ITQM) in the Zarb School of Business at the Hofstra University. He received his Ph.D. in Information Science from the University of Pittsburgh, a Master's degree in Telecommunications from the University of Colorado, Boulder, and a Bachelor's degree in Business Administration from Korea University. Prior to beginning his academic career, he worked for 6 years in telecom industry as research engineer. His main research areas are social network services in mobile networks, cyberspace and cyber security, radio frequency identification (RFID) in Hospital, and so on.