Feature Article

Cyber Security in Social Media: Challenges and the Way Forward

Kutub Thakur
Department of Professional Security Studies, Cyber Security; New Jersey City University

Jason Tseng
Department of Professional Security Studies, Cyber Security; New Jersey City University

Thaier Hayajneh
Department of Computer and Information Science; Fordham University

***Abstract*—This study highlights the issues relevant to current cyber attacks on social networks, challenges, and the possible ways to thwart the cyber criminals from accessing the social networks and causing damage. Finally, it presents important recommendations for preventing the social network from cyber attacks for better understanding of the field.**

In the recent past, cyber space has touched almost everyone and everything. In spite of developments in cyber security—the body of technologies, practices, and processes designed to protect computers, programs, data, and networks from unauthorized access or attacks—cyber information and resources are never fully secured against cyber attacks. It has been realized that within a very short time span, millions of attacks can be launched in the cyberspace, and the analysts of ensuring cyber security need to be constantly alert.[1]

Digital Object Identifier 10.1109/MITP.2018.2881373
Date of current version 27 March 2019.

More recently, online social networks became wildly popular. Social media represent "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content."[2] Using platforms like Facebook, YouTube, Twitter, LinkedIn, Instagram, Snapchat, etc., billions of people are building online communities and connecting with each other. These web platforms offer novel opportunities for socialization and interaction among the users, which have transformed the way users share information, like personal data, news, opinions, as well as successful conduct online businesses.[3]

Published by the IEEE Computer Society

Due to the inherent nature of social media, people are becoming easy prey of cyber criminals in this channel. Organizations are increasing IT budgets to safeguard social networks around the world. It has been observed that an overwhelming amount of information is created and shared by users through the social network. It is urgently required to adopt a new set of tools and techniques for securing online information and resources through social networks.

Following the Introduction section, "CYBER SECURITY: CURRENT PERSPECTIVES" and "SECURITY MODEL" provides the current perspective of the cyber security and an effective model for ensuring cyber security. "CYBER THREATS IN SOCIAL MEDIA" highlights the major attack vector in the social media. "CHALLENGES FOR CYBER SECURITY IN SOCIAL MEDIA" provides the most critical challenges in ensuring cyber security. "EFFECTIVE MEASURES FOR CYBER SECURITY IN SOCIAL MEDIA" provides the important recommendations and effective measure for maintaining the security information over social media networks. Finally, "CONCLUSION" presents the conclusion.

CYBER SECURITY: CURRENT PERSPECTIVES

Social networks like Facebook, Twitter, etc., play a vital role in communication among the users in the recent years. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also give the same power to spread false information, which can be just as damaging. The rapid spread of false information through social media is among the emerging risks identified by the World Economic Forum in its Global Risks 2013 report.[4]

The point is that cyber criminals can now weaponized social media sites and their data, leading to some of the biggest data breaches over the last few years.[5] For example, LinkedIn was a key tool for reconnaissance (the scraping of public social data and social engineering tactics) for the cyber criminals who executed Anthem Health's 2015 breach and its 80 million stolen records, while Twitter was an integral component of an innovative malware exploit dubbed "Hammertoss." This technique has even been rumored to be connected to the Pentagon's data breach last summer that took down the security agency's 4200-employee email server for two weeks while undetermined amounts of data were stolen.

In spite of many academic and industrial efforts for ensuring cyber security, issues are becoming increasingly more common. Issues such as data breaches at the prominent retailers Neiman-Marcus and Target, fundamental flaws in security protocols like the OpenSSL Heartbleed Bug and the successful government agencies attacks by hacktivist groups. According to the Data Breach Investigation Report by Verizon in 2015, there were more than 100 000 confirmed cyber security incidents in the year before, which resulted in the financial loss of $400 million. This confirms the relentless efforts of the hackers, as well as the vulnerability of the cyber security defense mechanisms.

New threats and challenges are also emerging continually with emerging technologies like IoT, Big Data *etc*.[6] The incidences of spear phishing are also increasing that involve the installation of harmful malware on the computer of the targeted users and stealing valuable and sensitive information. The installed malware can and may encrypt files on network drives, databases, and backups, thus causing serious damage to the target organization. The malware maybe distributed via ads on major websites. Again, state actors are increasingly using digital tools, often for achieving their strategic objectives, as well as for resolving or supporting conflicts, as identified by intelligence agencies.[7]

Cyber criminals are targeting individuals as well as companies through phishing emails. The phishing emails are used for installing ransomware. The same can also be spread via hacked or compromised web pages. This ransomware encrypts the important files of the victims, causing damage to the particular software, and messages from the criminals are displayed. Even in some cases, hospitals or care facilities are being targeted, where maintaining continuity is highly necessary. The rate of ransoms also depends on

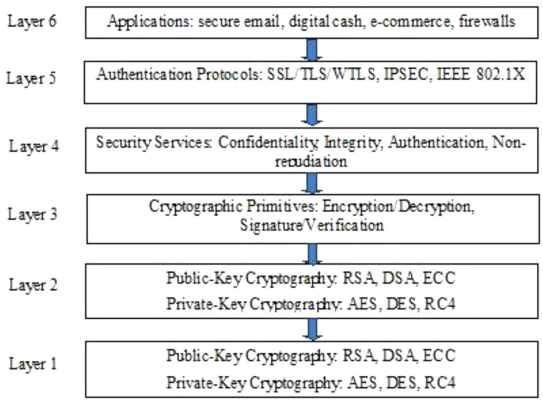

Figure 1. Six-layer hierarchical model for information security applications.

the type of organizations or persons, and the security personnel and cyber experts are finding it difficult to protect them.[7]

In addition, attacks like denial of service can prevent or slow legitimate users from accessing a system. These sorts of attacks are increasing at an alarming rate at present times. Using cyber theft or cyber espionage, the cyber criminals are being benefited from the financial, personal, or proprietary information of a person. Using botnet malware, the cyber criminals are trying to gain control of particular systems. In fact, it can be concluded that the confidentiality, availability, and integrity of Internet based information system and the information are regularly being compromised by a successful cyber attack.[8]

Particularly, security risks associated with social networks are increasing day-by-day. Improper uses of social media involving the information disclosure and different privacy issues are always harming the innocent users. In addition, online fraudsters, phishers, and sexual predators are regularly using the vulnerabilities of social media networks and causing serious damages. They are using improved tools and techniques to target the social media users, who are unable to confirm or resolve the issues of privacy and trust within the social media networks.

SECURITY MODEL

In order to achieve information security in the cyber space and protect valuable data in computers and communication networks from unauthorized access or modification, a six-layer model has been implemented, which is based on cryptographic algorithms,[9] as depicted in Figure 1. While analyzing the security model from top to bottom, it can be observed that the top most layer interact a number of prominent security applications like digital cash, secure e-mail, firewalls, *etc*. These applications rely on implementing the secure authentication protocols like IPSec, secure socket layer (SSL)/TLS, etc., at layer 5. These protocols also need the implementation of layer 4, which contains customary security services like integrity, confidentiality, authentication, and nonrepudiation. These security services are strengthened by two pair of cryptographic primitives as shown in layer 3, e.g., encryption/decryption and digital signature/verification. These also need the combination of private-key and public-key cryptographic algorithms depicted in layer 2, like RSA, AES, DES, etc. It is also necessary to implement an arithmetic operation so that high performance can be obtained from the cryptographic algorithms.

CYBER THREATS IN SOCIAL MEDIA

While social media sites may not create completely new cyber threats, they do substantially amplify the risk of existing ones.[5] From reconnaissance to brand hijacking and threat coordination, cyber criminals have been using social media to boost the effectiveness of their attacks for years. It is clear that social media risk is not solely about brand and reputation damage but is a sinister cyber security threat that can lead to major data breaches, numerous compliance issues, and large amounts of lost revenue due to fraud and counterfeit sales, along with a slew of other risks. The major threats in social media are highlighted in the following.

Social Engineering Attacks

Cyber criminals are heavily utilizing social engineering for eliciting the personal information of individuals by using fake social media accounts and building trust over the time.[10] This information may include name of the projects being involved with the individuals, name of the servers, *etc*. Compounding the issue is the use of

online collaboration and communication tools and the growing trend toward Bring Your Own Device policies.

Recent attacks on RSA and New York Times have proved that social engineering attacks can be effectively conducted through targeted spear-phishing. Users trust their partners in social media and often share highly sensitive information through this channel. This may result in leaking that information. As the social media users they are vulnerable, this social engineering has become one of the most serious threats in virtual communities. Even the most sophisticated corporate entities are becoming the easy targets of the adversaries through social engineering, who try to convince them to disclose sensitive information.[11]

In any engineering attack on social media, the major steps involved are as followed:

1. information gathering;
2. examination of social networking media;
3. tailored social engineering;
4. sensitive insider information.

There exist different types of malware like active contents, scripts, executable code, or other kind of software, which can be used to gather sensitive information by gaining illegal access to the system. According to a recent survey, 70% of malware exist in social media, especially on Facebook, Myspace, Twitter, and LinkedIn.[10]

Social media websites can also become vulnerable due to different tactics. These may include cross-site scripting (XSS), click jacking, baiting, phishing, phreaking, doxing, scams, and spoofing.[10] Due to immense popularity, social media websites have become the best destinations for the cyber criminals to conduct criminal activities. Social media websites also allow users to run third-party applications like games, which may lead to additional vulnerabilities.

Social Networking Sites

Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements and via third-party apps.[13] On Twitter, shortened URLs (popular due to the 140-character tweet limit) can be used to trick users into visiting malicious sites that can extract personal (and corporate) information if accessed through a work computer. Twitter is, especially vulnerable to this method because it is easy to retweet a post so that it eventually could be seen by hundreds of thousands of people.

Lack of a Social Media Policy

Distaster is waiting for any enterprise without social media policy or guidelines. Employees cannot be expected to represent the company on social networking platforms without proper training. The goals and parameters of the enterprise's social media initiative should be clearly stated. Who is allowed to use social media on behalf of the organization and what they are allowed to say are the two most obvious questions that must be addressed in a social media policy. Two more imperatives related to social media policy are as follows.

1. Organizations must conduct proper training for employees, if only to clear up issues regarding official social media policies.
2. A social media initiative needs a coordinator and champion, and that means a social media manager.

Spam and Scams

Social media websites, like Facebook and Twitter, can be the easy targets of cyber criminals to conduct heinous cyber crimes. Using exciting posts like celebrity talks, cyber criminals try to attract Facebook users, which gives them opportunities to conduct spam or phishing attacks. These attacks can also be done through the chat features of Facebook. Cyber criminals also use short promotional posts on Twitter to spread malware. In addition, the compromised social media accounts can give the spammers the chance to send spam messages to other users and harm the other users.[14]

Furthermore, the brand reputations of social networks are often misused for boosting the credibility of bulk mails sent outside of the social media. For instance, spoofed emails that claim to come from the support center and notify users about password resets or new friend requests are increasing at an alarming rate. Targeted emails are being sent with a template messages

like "Dear user of Facebook, because of the measures taken to provide safety to our clients, your password has been changed. You can find your new password in the attached document. Thanks, Your Facebook."

Other threats in social media may include targeted spam, follower scams, impersonation of celebrities and friends, phishing, defamation, cyber bullying, XSS, CSRF, *etc*. For instance, if a victim fails to recognize a defamations attack immediately, he or she may fail to access the offending content, and may have to face the inevitable consequences. Cyber bullying on social network includes denigration, harassment, sharing someone's secret information or images unlawfully, stalking, exclusion, threatening, etc. A subform of cyber bullying includes publishing personal information, even including phone numbers, home addresses, or class schedules. They may act as a source of additional social threats.[3] Parents have also been concerned about the opportunities available in social media for sexing or child pornography. Using sexually explicit text messages or other sexually explicit contents, people, particularly teens, are being harassed. All of these have resulted in serious cyber crimes involving the social media networks.

Security Risks of Mobile Social Media

The popularity of accessing social media using mobile devices is increasing rapidly, which has also attracted the attention of the cyber criminals. The frequency and sophistication of malware and virus attacks are also increasing, causing a variety of damages, like leaking of user privacy, battery power depletion, information theft, and financial loss.

It has been identified that in most of the cases, mobile devices have weaker defense mechanisms than the PCs. Furthermore, according to Kaspersky Labs, social media sites can be more vulnerable to malware than the email exchange websites. Hence, social media network can pose a variety of security risks to the users of mobile devices.[2]

Smart phone users can be easily hit by Android malware by downloading the marketplace applications that carry malicious code. Some of the malware has the power to reveal the private information of the user, or even destroy the user data. As Android operating system, is an open-source software stack, the mobile phones powered by Android can be easily targeted by malware.

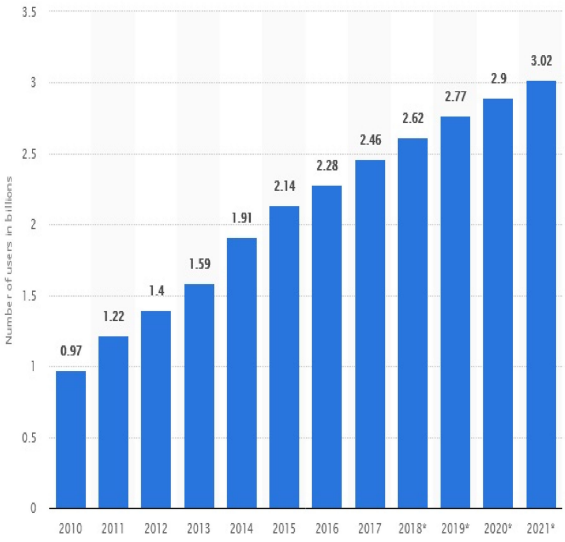

Figure 2. Number of social media users worldwide from 2010 to 2021 (in billions).

Many employees of business organizations store sensitive corporate information on their mobile devices and access that information with these partially secure devices. Through social media, this information can be leaked when these are shared inadvertently. Furthermore, attacks like "TCP sequence number inference attack" can harm a mobile phone user by allowing a harmful malware to hijack a Facebook connection, replace the login page, or inject malicious Java Scripts for posting a new status on behalf of the victim user.[2]

CHALLENGES FOR CYBER SECURITY IN SOCIAL MEDIA

Social networks have become a common medium of communication and sharing sentiments. The number of users throughout the world is continuously increasing day-by-day. It has been predicted that in 2021, the number of user on social network will cross three billion, which is more than thrice than that of 2010, as depicted in Figure 2.[15]

This increasing trend of number of users of social networks has also lead in a tremendous

increase in security flaws that cause the effect on users' security objectives like confidentiality, integrity, and privacy.

The major challenge involved in ensuring cyber security in social media is the vulnerability of the social network security systems.[14] Vulnerabilities of Facebook applications may allow a cyber criminal to conduct attacks on the private data of the users. In most of the cases, these are CSRF or XSS types of attacks, which may lead to data breaches.

Social media networks often allow various applications to access user data through a variety of interfaces, which can be harmful. Challenges emerge due to the conflicting needs of the social media users. On one hand, they want to ensure privacy, and on the other hand, they like to share more and connect with as many friends as possible.

People may put themselves and those connected with their social network at risk simply by putting a variety of personal or other sensitive information on their social media profiles, often about their passions and interests that may be easily accessible to the cyber criminals. Spammers, stalkers, and hackers can use this information for their own benefits.[16]

From an organizational perspective, challenges arising from naïve social media actions of employees represent a greater threat to information security. Moreover, employees are often confused in their professional and personal roles when collaborating and communicating with coworkers and customers in social media, which also poses security risks. These risks compounds when the employee holds a higher position in the organization. Employees often communicate with their colleagues through social media, which may not be steered by the company. This may also represent an information security challenge.[17]

EFFECTIVE MEASURES FOR CYBER SECURITY IN SOCIAL MEDIA

The first thing that one must come to terms with is that social networks cannot secure their own environments, let alone yours. As much as they aim to mitigate security threats and issues on their platforms, they are nowhere close to 100% effective. Facebook reported that for 2015 up to 2% of its monthly average users (31 million accounts) are false. Twitter estimates 5%, and LinkedIn openly admitted, "We don't have a reliable system for identifying and counting duplicates or fraudulent accounts."[5]

The following measures help to ensure the cyber security in the social media.

I. Social media users should be careful before sharing anything with other users in order to ensure privacy and security. Most social media websites let the users set different privacy settings. They can decide with whom to share their information, like "friends," "friends of friends," or "everyone" as in Facebook.
II. The users must keep following points into consideration as effective steps to ensure safe digital communication, particularly in social media:[18]

A. Keep personal information personal.
B. Think before click: Download safely and legally.
C. Buyer beware: Shopping safely and carefully.
D. E-mail: Open it carefully, send it thoughtfully.
E. Chat safely and responsibly.
F. Control the camera.
G. Do not overshare.
H. Observe proper social networking etiquette and safety precautions.
I. Keep it short and know your place: Using microblogging and location-based services.
J. Control, filter, and protect: Optimizing the use of controls, filters, and antivirus programs.

III. Installation and updating of security software such as firewalls and antivirus are essential on mobile devices as well in order to avoid malicious apps and different other threats. Security professionals need to implement secure gateway technologies that offer network packet filtering and antimalware capabilities, which can be vital for reducing the risks of data loss and malware infection.

Proper steps should also be taken regarding the integration of data loss prevention (DLP) solution with mobile devices and social media, which allow the enterprises to monitor and control the flow of sensitive data on the network. This can be effective for encrypting confidential

contents, preventing the loss of sensitive data, and averting malware. For instance, a DLP solution can display a pop-up warning message when a particular social media policy is violated.

IV. Training and awareness can be immensely helpful to keep the social media users safe from the cyber criminals. Particularly, the employees of different business organizations need to be properly trained and advised of social engineering initiatives. The overall impact of these training programs can be increased by making them personalized and scenario-based.

People should be aware that they can be protected from the harm of infiltrators by limiting the amount of personal and professional information they make available on the social networking websites, not accepting the less secure default security and privacy settings of their social media page, and not accepting friend requests from unknown sources.[12]

Furthermore, organizations should develop personalized, interactive, and engaging approaches, as well as add behavioral science issues in their information security training and education programs, and try to foster information security culture within the organizations.[2]

V. Social media users can enable secure connection options, which use HTTPS, i.e., the combination of HTTP and SSL, in lieu of simple HTTP.[10] In HTTPS, pages coming from social media, like Facebook, Twitter, or LinkedIn add some protection layers by encrypting the data. This can help in adding more protection to the social media websites.

To truly build a comprehensive social media security plan, one needs to include external risk factors and threats outside of IT control. These can include brand impersonations and physical security threats to your employees or top executives. This should be done while also seeking feedback company-wide and coordinating with a range of stakeholder across legal, compliance, operations, and finance to ensure that all bases are covered.

In a nutshell, some of the challenges that most of the countries worldwide is currently dealing with in regards to cyber security, particular to social media include the following:

- the need for more collaboration in order to mitigate threats;
- education and awareness;
- the balance between privacy and security.

CONCLUSION

Billions of people want to interact with others through social media, and it has also become a new attack ground for the cyber criminals. Through spreading malicious code and sending spam messages, they are trying to take advantage of the inherent trust of the users in their relationship network.

Hence, privacy and security in the social media networks have become the main concern of the users. Social media websites need to recognize the basic aspect of human social interaction and identify intuitive and strong methods to ensure the required levels of privacy, protection, and trust. Governments, intelligence agencies, and technology experts must come forward and try to adopt new technologies and paradigms for using and manipulating the amount of information in a social Web.

In addition, cyber security should not be treated as optional, but it must be a part of the design of every product, database, and electronic communication. One can play a significant role to secure our future, particularly in social media by education, spreading the awareness for creating a balance between privacy and security and incorporating proactive changes in our policies.

REFERENCES

1. M. McNeese *et al.*, in *Proc. Human Factors Ergonom. Soc. Annu. Meet.*, Los Angeles, CA, USA, 2012, vol. 21, pp. 268–271.
2. W. He, "A survey of security risks of mobile social media through blog mining and an extensive literature search," *Inf. Manage. Comput. Secur.*, vol. 21, no. 20, p. 381, 2013.
3. A. M. de Paula, "Security aspects and future trends of social networks," in *Proc. 4th Int. Conf. Forensic Comput. Sci.*, Jan. 2009, pp. 66–77.

4. B. Goodwin, "Misuse of social media could wreak havoc," 2017. [Online]. Available: http://www.computerweekly.com/news/2240175704/Misuse-of-social-media-could-wreak-havoc- warns-WEF
5. N. Hayes, "Why social media sites are the new cyber weapons of choice," 2017. [Online]. Available: https://www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons- of-choice/a/d-id/1326802?
6. S. D. Pawlowski and Y. Jung, "Social representations of cybersecurity by university students and implications for instructional design,"*J. Inf. Syst. Educ.*, vol. 26, no. 4, p. 281, 2015.
7. W. Oosterbaan, *Eur. Cyber Secur. Perspectives*, 2017. [Online]. Available: https://www.tno.nl/media/9401/european cyber security perspectives 2017.pdf
8. N. Rao, "GSM-R global system for mobile communication-railway," *CSI Commun.*, p. 13, 2012.
9. F. Rodríguez-Henríquez, N. A. Saqib, A. D. Perez, and C. K. Koc, *Cryptographic Algorithms on Reconfigurable Hardware*. Berlin, Germany: Springer, 2007.
10. H. A. Gohel, "Cyber security and social media," *Know Your CSI*, p. 33, 2015.
11. M. J. Teplinsky, "Fiddling on the roof: Recent developments in cybersecurity," *Amer. Univ. Bus. Law Rev.*, vol. 2, p. 225, 2012.
12. J. J. Lenkart, "The vulnerability of social networking media and the insider threat: New eyes for bad guys," Ph.D. dissertation, Naval Postgraduate School, Monterey, CA, USA, 2011.
13. C. Nerney, "5 top social media security threats," 2011. [Online]. Available: https://www.networkworld.com/article/2177520/collaboration-social/5-top-social-media-security- threats.html
14. C. Wuest, "The Risks of Social Networking," Symantec Corporation, Mountain View, CA, USA, 2010.
15. Statista. "Number of social media users worldwide from 2010 to 2021 (in billions)," 2017. [Online]. Available: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
16. P. Gundecha and H. Liu, "Mining social media: A brief introduction," *New Directions in Informatics, Optimization, Logistics, and Production* (Informs, 2012), pp. 1–17.
17. R. Hekkala, K. Väyrynen, and T. Wiander, "Information security challenges of social media for companies," *ECIS*, p. 56, 2012.
18. T. B. Orr, *Top 10 Tips for Safe and Responsible Digital Communication*. New York, NY, USA: Rosen, 2012.
19. McAfee. "10 tips to protect yourself on social networks," 2014. [Online]. Available: https://securingtomorrow.mcafee.com/consumer/family-safety/10-tips-protect-social-networks/

Kutub Thakur is an assistant professor and the director of cyber defense and security program of New Jersey City University. He also worked as an adjunct assistant professor of City University New York. He worked for various public and private entities such as Lehman Brothers, Barclays Capital, ConEdison, the United Nations, and the Metropolitan Transport Authority. His research interests include cybersecurity, forensics, and machine learning. He has authored or co-authored several scientific journals, book chapters, and conference publications. He is certified in computer hacking and forensics investigation. Contact him at kthakur@njcu.edu.

Thaier Hayajneh is the founder and the director of the Fordham Center for Cybersecurity, University Professor of Computer Science, the program director of MS in Cybersecurity at Fordham University, New York, NY, USA. He was a full-time faculty of computer science at New York Institute of Technology and the founding director of NYIT Center of Excellence in Cyber Security (2014–2016). His research focuses on cybersecurity and networking, including wireless security, applied cryptography, blockchain, and cryptocurrency. He has authored or co-authored more than 70 papers in reputable journals and conferences. He received the Ph.D. degree in information sciences with specialization in cybersecurity and networking from the University of Pittsburgh, PA, USA, in 2009 and 2005, respectively. He served on several NSF Cybersecurity review panels and serves as a CAE reviewer and a mentor for NSA. He is serving as the editor in chief for *EAI Endorsed Transactions on Pervasive Health and Technology*, an editor for *ACM/ Springer Wireless Networks*, and a guest editor for other prestigious journals. He has served as the program chair on the technical program committee of several leading conferences, including IEEE NSS, GLOBECOM, and ICC. He has reviewed for several prestigious journals (over 100 reviews) and received Sentinels of Science as a peer review award from Publons. Contact him at thayajneh@fordham.edu.

Jason Tseng is an adjunct assistant professor with New Jersey City University. He has 20 years of professional IT experience, where he has held positions from IT Support Engineer to IT manager. His research interests include virtualization, cloud computing, hosted services and management, data center management, disaster recovery, and information security. He has authored or co-authored several journals and has presented at many conferences. Contact him at Jtseng@njcu.edu.