Yuhong Liu and Yan (Lindsay) Sun

Securing Digital Reputation in Online Social Media

As computing and communication systems evolve rapidly and ubiquitously, it has become convenient and almost effortless for individual users to generate, share, and exchange information on online social media. Through online social media, a wide range of digital content, which covers blogging, forums, reviews, social networking, question-answer databases, digital video, mobile phone photography, and wikis, is created by users and has dramatically changed the way people work and interact. However, the simplicity of creating such digital content online has also led to an increase of users' concern about the trustworthiness of such information. To address the issue of trustworthiness, a widely recognized approach is to evaluate the quality of the online information based on feedback from large scale, virtual word-of-mouth networks where individuals share their own opinions and experiences. The aggregated result of such feedback is called *digital reputation*. Digital reputation has already been widely adopted by current online social media. For example, viewers on YouTube may "like" or "dislike" a video clip, buyers on Amazon share their purchasing experiences, travelers evaluate hotels or restaurants on Yelp, and readers can either "dig" or "bury" a piece of social news on Reddit. The reputation-based solution is playing an increasingly important role in influencing users' online social interactions. For example, eBay sellers with established reputations can expect about 8% more revenue than new sellers marketing the same goods [1]; the survey in [2] reveals that the services receiving five-star ratings will attract 20% more revenue than the same services receiving four-star ratings.

Driven by the increasing profits in online social media, manipulations against digital reputation systems are gaining popularity, which in turn motivates security researchers around the world to prevent reputation manipulations. Most current studies focus on modeling various attacks and developing defense schemes and have already achieved some exciting results. Besides these well-studied attack and defense models, there are two under-investigated aspects: 1) how to obtain reliable data for investigating attack and defense in online reputation systems and 2) how to understand the impact of real-world reputation on digital reputation security. We briefly review the current studies of reputation attack and defense models and then discuss in details these two underinvestigated aspects.

ATTACKS AND DEFENSES IN DIGITAL REPUTATION SYSTEMS

REPUTATION ATTACKS

Due to the increasing impact of reputation systems on individual users' online social interactions, the incentive to manipulate digital reputation is growing. For example, some eBay users are artificially boosting their reputation by buying and selling feedback. On IMDB, a movie named *Resident Evil: Afterlife* had kept an overly inflated reputation score of 8.5 out of 10 with more than 1,800 ratings during its first month of release, whereas its reputation fell down to only 5.9 after the promotion period. For just US$9.99, a company named "Increase YouTube Views" can provide 30 "I like" ratings or 30 real user comments to video clips on YouTube. Weibo, the microblog in China where users can follow others as "fans," is one of the most popular social Web sites with billions of users. Some companies are making profits by selling millions of "zombie fans," which are automatically generated fake accounts, to boost customers' popularity. Recently, many online businesses that provide diverse "reputation repairing" services are emerging and gaining popularity. So-called professionally trained writers are provided to write positive reviews/articles and spread them all over the social Web sites, blogs, and forums to repair or boost the reputation of individual customers. The business customers can pay to eliminate/suppress negative reviews, such as bad ratings on the Better Business Bureau Web site (www.BBB.com) and ComplaintsBoard.com, and receive positive reviews on different reputation Web sites, such as Yelp, Google Places, CitySearch, Amazon, and TripAdvisor.

Many scientific studies have been conducted to investigate possible attacks against reputation systems. In [3], many existing attack approaches have been summarized according to their evolution trend, from simple to complicated attacks. For example, the simplest attack is the whitewashing attack where an attacker simply discards its disreputable identification (ID) and re-enters the system by registering a new ID with fresh reputation. A slightly more complex attack is the traitor attack, where an attacker restores reputation by performing good behaviors and then behaves badly again. In advanced attacks, such as sybil attacks,

Digital Object Identifier 10.1109/MSP.2013.2282414
Date of publication: 5 December 2013

the attacker registers multiple user IDs to collaboratively provide unfair feedback. One of the most recent attack models, RepTrap [4], can overturn the reputation of a large number of online items (from positive to negative) and undermine the fairness of the entire reputation system. These studies have shown that reputation attacks may greatly distort reputation scores, undermine users' confidence in the fairness of the reputation systems, and lead to unfair business practices.

REPUTATION DEFENSES

Extensive reputation defense studies have been done from online feedback (i.e., online ratings/reviews) anomaly detection and user-behavior modeling. Studies from the former aspect consider user ratings as random variables and assume dishonest ratings to have statistical distributions different from normal ratings. The approach in [5] assumes that the normal ratings follow a Beta distribution and identifies the ratings outside the majority's opinions as dishonest ratings. In [6], dishonest ratings are eliminated through controlled anonymity and cluster filtering. The defense approaches focusing on user behavior modeling include the iteration refinement approach proposed in [7], which computes the "judging power" for each user as the inverse of this user's rating variance. Users with larger judging power have higher weights in reputation calculation. A personalized trust model is proposed in [8] to enable customized trust evaluations for different users. An in-depth survey on defense approaches can be found in [3].

SUMMARY

Reputation attack and defense studies are developing rapidly. The evolution of one side will inspire the development of the other, and there is always an "arms race" between the reputation attack and defense schemes. Although the reputation attack and defense studies have attracted much research attention, there are still two challenging issues not fully investigated: 1) to obtain reliable and real attack data for studying reputation attacks and defenses and 2) to understand how the digital reputation interacts with the real-world reputation.

DATA COLLECTION

The collection of real user attack data is important for both the study of reputation attack strategies and the evaluation of reputation defense schemes. However, it is costly and inefficient to collect attack data by arbitrarily crawling online social media and manually identifying attacks. It is also extremely difficult to obtain the ground truth of such data (i.e., whether a piece of feedback is honest or dishonest). Therefore, many studies rely on simulated data [5], [7], [8]. However, the simulated data often only represents a few types of attacks, which may have already been considered in the design stage of the defense schemes. Such an evaluation may not reflect the defense performance in practical settings, where attackers may develop diverse and even unknown attacks. The lack of realistic attack data is surely a hurdle in reputation security research.

To address this issue, one promising approach is to collect data through crowdsourcing, where we can launch open calls to an unknown group of solvers (i.e., a crowd). Companies and institutions can use crowdsourcing to help their decision making, problem solving, and data collection. There are four advantages to collect attack data through crowdsourcing: 1) the cost is relatively low; 2) it is much easier to discover the ground truth, if we provide normal data (i.e., honest feedback) and ask the crowd to provide attack strategies; 3) the collected attack strategies are generated by real human users and are therefore more realistic, and 4) more diverse attack strategies can be obtained due to the different knowledge background of the crowd. These advantages make crowdsourcing a promising approach to collect data for reputation research.

A COMPETITION CROWDSOURCING: CANT COMPETITION

The Challenge-of-Attack-on-Network-Trust (CANT) was launched in 2008 to collect reputation attack data. In the competition, we built a virtual reputation system with normal rating data. The crowd (i.e., players) was required to provide attack strategies to downgrade the reputation score of a given product as much as possible, and the winners received cash rewards. The competition lasted for 18 days and attracted more than 630 registered players with 826,980 valid submissions. The collected data set has provided rich information for investigations of the real user attack behaviors and served as testing data set to evaluate the attack-resistance properties of reputation defense schemes. Figure 1 is the user interface of the CANT competition.

In the competition, each player registered one and only one player ID, which was used to track the player's submissions, score, and rank. Each player ID submitted attack strategies as many times as he or she could. In each specific submission, a player P could use u malicious user IDs to insert r unfair ratings, where $0 < u < U, 0 < r < R$. Here, U and R were the largest number of malicious user IDs and unfair ratings, respectively.

All submissions were divided into groups according to their u and r values. Specifically, the group $G_{u,r}$ contained all submissions that used u malicious user IDs and r unfair ratings. Within a group, the submission that yielded the strongest attack (i.e., downgrading the reputation score of product O_1 the most) was marked as the group winning submission. Note that there might be a tie, leading to multiple winning submissions in one group. Let $s_{u,r}$ denote the number of winning submissions in $G_{u,r}$.

In each group, the winning submissions equally split one point. If there was only one winning submission in $G_{u,r}$ (i.e., $s_{u,r} = 1$), the player who submitted the winning submission gained one point. Then, the overall score of a player was the sum of his/her winning submission points.

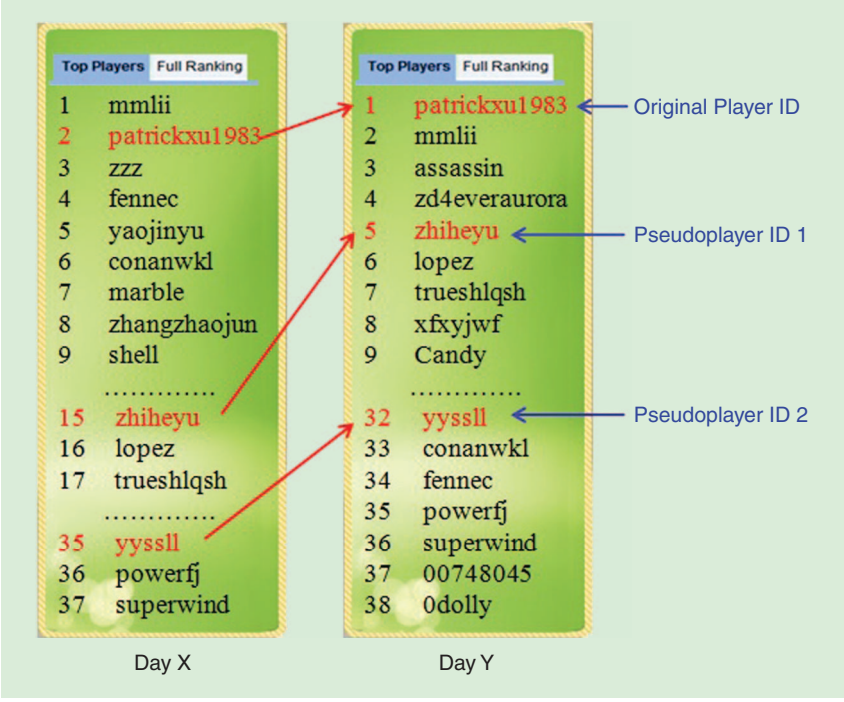
A CHALLENGING ISSUE: CHEATING BEHAVIORS

Surprisingly, cheating behaviors were found during the CANT competition. In

[FIG1] The user interface of the CANT competition.

particular, one player (denoted by cheater C) registered three player IDs. These player IDs had shared the same set of winning submissions and took second, fifth, and 32nd place, respectively, as shown in Figure 2. In the CANT competition, the top 19 players won cash prizes. By using pseudoplayer IDs, the cheater C could increase his rewards, if not detected.

How does such cheating behavior work? Assume that two players, P_1 and P_2, both have winning submissions in group $G_{u,r}$. Assume P_1 has one winning submission and P_2 has two. Without cheating, P_1 gets 1/3 points and P_2 gets 2/3 points, respectively in group $G_{u,r}$. Then, P_1 decides to cheat and registers a new player ID P_d. Through the new player ID P_d, the player P_1 can submit the same winning submission again. By doing so, $s_{u,r}$ is increased from three to four. Then, P_1 gets 1/4 point and P_2 gets 1/2 point. Before cheating, the difference between P_1 and P_2 is 1/3 point. After cheating, the difference between P_1 and P_2 is reduced to 1/4 point. Through the new player ID P_d, 1) the score gap between P_1 and P_2 is narrowed down, and the advantage of P_2 over P_1 is reduced; and 2) the player ID P_d grabs more points and gains a higher rank. This is exactly what happened in the CANT competition.



[FIG2] Rank boosting through multiple pseudo-IDs in the CANT competition.

[TABLE 1] PSEUDO-ID DETECTION RESULTS OF DIFFERENT SCHEMES.

	GROUND TRUTH	THE PROPOSED SCHEME	SCORE-BASED SCHEME
PSEUDO-ID	5, 32	5, 20, 32	5
ORIGINAL ID	2	2, 1	NONE

This type of cheating behavior can exist in other competition crowdsourcing cases, where competition rewards are provided. It is important to detect such cheating behavior since it will not only contribute no meaningful data/solutions to the system, but also ruin the fairness of the competition.

DETECTION OF CHEATING BEHAVIOR

We detect cheating behaviors in the CANT competition by building an implicit social network among players. Most existing social networks inherently describe collaboration among users (e.g., Facebook users who are connected are friends). Can the social network concept be used in a competition environment, in which nodes (i.e., players) have to defeat others to achieve their goals? We define a competition social network to describe such scenarios, in which the nodes' behaviors are dramatically different from these in collaborative social networks.

In the context of the CANT competition, we introduce the following concepts.

- A competition relationship exists and only exists between two player IDs when they have winning submissions in the same group (e.g., $G_{u,r}$).
- The competition value is computed for each pair of players with competition relationship. Assume $t^i_{u,r}$ denote the points obtained by player P_i in group $G_{u,r}$. We define

$$H^{i,j}_{u,r} = \begin{cases} 0 & \text{if } t^j_{u,r} \cdot t^j_{u,r} = 0 \\ 1 & \text{if } t^i_{u,r} \cdot t^j_{u,r} \neq 0 \end{cases}.$$

It is easy to see that $H^{i,j}_{u,r} = 1$ if and only if both P_i and P_j win points (or compete) in group $G_{u,r}$. The competition value from P_i to P_j and from P_j to P_i are

$$V_{pi \to pj} = \sum_{u=1}^{U} \sum_{r=1}^{R} t^i_{u,r} \cdot H^{i,j}_{u,r}$$

and

$$V_{pj \to pi} = \sum_{u=1}^{U} \sum_{r=1}^{R} t^j_{u,r} \cdot H^{i,j}_{u,r},$$

respectively.

- In the competition network, each player ID is a node. If two player IDs have competition relationship (i.e., $t^i_{u,r} \cdot t^j_{u,r} \neq 0$), there is a bidirectional link between them and two competition values are computed.
- The competition degree of a node is the number of links connected to this node in the competition network.

Although we focus on the CANT competition here, the concept of a competition network can be extended to other scenarios as long as one can define a quantitative competition value between two players. Ideally, the competition network can be updated whenever a new submission is received. To simplify the computation, we divide the overall time of the competition into 36 equal time frames, where one frame roughly represents a half day. We only update the competition network at the end of each time frame. We refer to the main ID controlled by the cheater as the *original ID* and to the other IDs controlled by the cheater as the *pseudo-IDs*. The goal is to detect the pseudo-IDs and their association with the original ID.

Unlike normal players whose winning submissions are accumulated gradually, pseudo-IDs usually share winning submissions from the original ID within a short time, leading to either a low competition degree (i.e., sharing only unpopular winning submissions) or a sudden increase in the competition degree (i.e., sharing popular winning submissions). The player IDs that fulfill either of these two conditions will be identified as pseudo-IDs. Furthermore, if the competition value between a player ID and an identified pseudoplayer ID is much larger than the average competition value, this player ID is marked as the associated original ID.

With the competition social network, we detect that Player 5 and Player 32 are the pseudo-IDs of Player 2, and Player 20 is the pseudo-ID of Player 1. We compare the proposed detection scheme with a simple score-based scheme, where a player is considered as pseudoplayer if his/her score suddenly increases. With a simple score-based scheme, we can detect Player ID 5 as a pseudoplayer ID, while the original ID cannot be detected. The results are shown in Table 1. The ground truth is obtained by interviewing players after the competition.

THE ROLE OF REAL-WORLD REPUTATION IN REPUTATION SECURITY RESEARCH

Although digital reputation is an important factor in influencing users' decision making, it is not the only one. Beyond digital reputation, users also make decisions based on the real-world reputation from the words of their friends, neighbors, and coworkers. Although the real-world reputation does exist, it has seldom been considered in the reputation security research, since the digital reputation is believed to be a dominant factor. The digital reputation may dominate in global markets where few users know each other. However, how about in a closely connected social community? Will the real-world reputation play an important role? If so, how will it influence the reputation security research?

COMPARING THE IMPACT OF DIGITAL REPUTATION AND REAL-WORLD REPUTATION

We discuss a study on mobile application (i.e., app) installation, in which both digital reputation and real-world reputation affect users' decision on whether to install an app. Similar to other markets, in the app market, people believe that the digital reputation heavily influences users' shopping decisions. Since app rating and download number are the two most important factors in the calculation of digital reputation, most manipulation is launched against these two factors. A well-known attack is the pay-per-install

model, where app sellers pay for each installation to boost the download number. Some companies, such as App Lifter, provide services for app sellers to directly pay users for installing their apps. Some other companies, such as Tapjoy and Flurry, manage pay-per-install networks composed of plenty of apps. Apps in such networks encourage their users through virtual currency or level upgrading to download other apps in the same network. App ratings/reviews can also be manipulated; for example, Molinker, the app developer with more than 1,000 apps, has been revoked from the app market due to a review scam [9].

On the other hand, with the popularity of tablet computers and smartphones, many users have experiences of installing mobile apps, and they often share such experiences with their local connections (e.g., friends, family members, colleagues). Thus, within a local community (i.e., university campus), apps may also have their real-world reputation, which provides us with an opportunity to evaluate the impact of the real-world reputation on users' decisions.

TESTING DATA

The testing data is a real user data set collected by the Massachusetts Institute of Technology Media Lab [10]. This data set records the installations of 821 apps from 55 participants, are residents living in a graduate student residency of a major U.S. university, from March to July 2010. In this data set, the following information has been collected:

- Users' app installation information (i.e., which user installed which app at what time).
- Call log and Bluetooth hits information. During the data collection period, each participant was given an Android-based cell phone with a built-in sensing software to capture all call logs and Bluetooth hits among the given phones. Call logs were used to indicate participants' interactions through phone calls. Bluetooth hits recorded participants' face-to-face interactions, during which the phones were within each other's vicinity. These two types of information described participants' daily interactions.
- Users' friendship, affiliation, and race information was collected through a survey. In the survey, each participant provided his/her affiliation and race and rated his/her friendship relationship to other participants. Such information reflected more about participants' long-term relationship.

This data set perfectly matches our requirements due to two reasons. First, it contains rich information about users' real-world interactions, i.e., call log, Bluetooth hits, friendship, affiliation, and race, which represents the real-world reputation. Second, users' app installation information, which is rarely available in other data sets, makes it possible to analyze the installation decision for each specific user. Beyond this information, we further collect the app rating and download number information to represent the digital reputation.

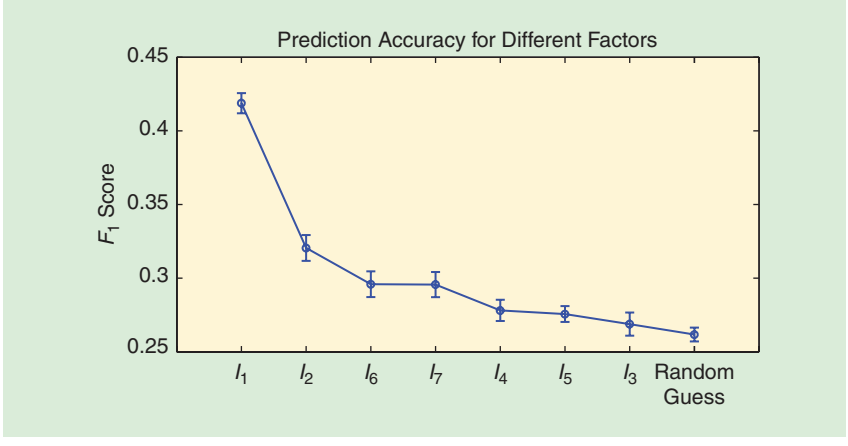
IMPACT OF DIFFERENT INFORMATION FACTORS

To evaluate the impact of different information on users' app installations, the first step is to accurately estimate app installations. We adopt the model in [10], which predicts app installations by constructing a composite network containing multiple sources of information. To the best of our knowledge, this is currently the most suitable model in terms of predicting app installations from diverse information sources.

In [10], the goal is to derive the optimized model to combine all the pieces of information so that users' app installations can be predicted with high accuracy. We use this model to understand which information has larger impact on users' app installations. The assumption is that if one factor has larger influence on users' app installations, the optimized prediction based on this factor should yield a higher accuracy. Therefore, each time, we take only one factor as the input to optimize the prediction model and calculate the prediction accuracy. The impact evaluation of different factors is based on the comparison of the prediction accuracy.

Specifically, to calculate the prediction accuracy, we adopt the F_1-score as the performance measurement, which is computed as $(2 \times \text{precision} \times \text{recall})/(\text{precision} + \text{recall})$. Here the precision is the number of correct results divided by the number of all returned results, and the recall is the number of correct results divided by the number of results that should have been returned. The optimal F_1 score is obtained by computing F_1 scores for each point on the precision-recall curve and selecting the largest F_1 value.

Figure 3 demonstrates the optimized prediction accuracy for each different factor. The y-axis represents the prediction accuracy (i.e., optimal F_1 score),



[FIG3] The impact of different information factors on the prediction accuracy (I_1: call log; I_2: Bluetooth hits; I_3: friendship; I_4: affiliation; I_5: race; I_6: app download number; and I_7: app rating).

and the x-axis represents different input factors. From Figure 3, we can make several observations:

- Compared to random guess, where no information is available, all these factors achieve higher F_1 scores thus suggesting that each of these factors will provide some information for the app installations. In other words, all of these factors have impact on users' app installations.
- Prediction with call log information yields the highest F_1 score, indicating that call log has more impact on users' app installation decisions than other factors. If a user has many frequently called friends who have installed a certain app, the call-log number for this user and this particular app is high. The detailed computation of call-log and other factors can be found in [10].
- The daily interaction information, i.e., call log and Bluetooth hits, has a much higher impact compared to the long-term relation information, such as affiliation, race, and friendship. This suggests that users' app installations may easily be influenced by people who contact them every day. Even if two users are friends, if they do not contact each other frequently, their impact on each others' app installations is limited.
- The impact of app rating and download number, which represents the digital reputation, is lying in the middle thus suggesting that to install apps, users in a closely connected social community, such as a university campus community, may first refer to people whom they contact frequently, then check out rating/download information that is publicly available, and at last refer to other people who are in the community but have less frequent contact.

Based on these observations, it seems that in a closely connected social community, the real-world reputation has larger impact than the digital reputation. Furthermore, among different social connections, users tend to be influenced more by their frequent contacts. Note that this study is based on the data from a very special community, a university campus and may not generalize to a broader consumer base.

THE ROLE OF THE REAL-WORLD REPUTATION ON REPUTATION SECURITY RESEARCH

The experimental results shown above suggest that when a person knows his/her friends' opinion about an app, this person will pay much less attention or even ignore the online reviews and ratings. Although the real-world reputation has rarely been considered in the reputation security research, it is the dominant factor in influencing users' decisions in a closely connected social community. Then how will this influence the reputation security research? We would like to discuss it from both the attack and the defense perspectives.

A GOOD UTILIZATION OF THE REAL-WORLD REPUTATION CAN WELL COMPLEMENT THE DIGITAL REPUTATION AND HELP IMPROVING ITS ATTACK-RESISTANCE PROPERTIES.

From the attack perspective, to influence users' decisions in a closely connected social community, manipulating the real-world reputation may be more effective than manipulating the global digital reputation. Therefore, the pay-per-install model may not be a good attack strategy for a closely connected social community. On the other hand, the app developers are suggested to advertise their apps on online forums, blogs, and social networks (e.g., Facebook, Twitter) to boost their real-world reputation and cultivate potential customers. Although such promotions are usually more costly and take longer, they may be more effective than manipulating the digital reputation only.

From the defense perspective, the designer takes advantage that real reputation overwrites digital reputation in closely connected social communities. For example, if the designer can identify the users who belong to the same closely connected social community (e.g., university campus) and capture the reputation of an app in this community (e.g., ratings from this community), the designer can then investigate whether this local reputation agrees with the global digital reputation. Any significant difference may lead to further investigation. Another interesting direction is to make the real-world reputation more accessible. A user may benefit from a more personalized reputation system that considers this user's social community. Given these, we believe that a good utilization of the real-world reputation can well complement the digital reputation and help improving its attack-resistance properties. This will be an interesting direction for future research.

SUMMARY

In this column, we have discussed security issues of digital reputation in online social media. In particular, digital reputation has already been proven to be an effective approach to ensure information quality in the rapidly developing online social media. Driven by the low costs and large potential profits of manipulating digital reputation, diverse attacks are emerging, which attracts much research attention. However, due to the lack of realistic attack data, the evaluation of the reputation defense schemes has been a challenging task. A promising approach is to collect the real user attack data through crowdsourcing. Unexpectedly, cheating behaviors may also exist in the crowdsourcing process. To address this issue, we described a "competition social network" to effectively model the crowd's behavioral patterns and to detect anomaly. Finally, we have compared the digital reputation and the real-world reputation, and believe that the integration of the two types of reputation will be an interesting direction for research aiming to provide secure and trustworthy reputation in online social media.

RESOURCES

- Everything you need to know about eBay feedback. [Online]. Available: http://www.newlifeauctions.com/feedback.html

■ R. Kalla. IMDB, Whats going on with your scores? [Online]. Available: http://www.thebuzzmedia.com/imdb-whats-going-on-with-your-scores/

■ Increase views and ratings on YouTube videos. [Online]. Available: http://www.earnersblog.com/increase-youtube-video-views/

■ S. Millward. Of Sina Weibo's 500 million registered users, Are 90% actually zombies? [Online]. Available: http://www.techinasia.com/sina-weibo-90-percent-users-zombies/

■ Reputation repair. [Online]. Available: http://www.reputationchanger.com/

■ App Lifter. [Online]. Available: http://applifter.com/

■ Tapjoy. [Online]. Available: http://developers.tapjoy.com/how-it-works/

■ Flurry. [Online]. Available: http://www.flurry.com/appCircle-a.html.

ACKNOWLEDGMENT

This research was sponsored by the National Science Foundation under award 0643532.

AUTHORS

Yuhong Liu (yuhong@ele.uri.edu) is an assistant professor at Penn State, Altoona.

Yan (Lindsay) Sun (yansun@ele.uri.edu) is an associate professor at the University of Rhode Island.

REFERENCES

[1] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of Ebay's reputation system," in *The Economics of the Internet and E-Commerce* (Advances in Applied Microeconomics, vol. 11). Amsterdam, The Netherlands: Elsevier, 2002, pp. 127–157.

[2] comScore Inc. and T. K. Group. (2007, Nov.). Press release: Online consumer-generated reviews have significant impact on offline purchase behavior. [Online]. Available: http://www.comscore.com/press/release.asp?press=1928

[3] Y. L. Sun and Y. Liu, "Security of online reputation systems: Evolution of attacks and defenses," *IEEE Signal Processing Mag.*, vol. 29, no. 2, pp. 87–97, Mar. 2012.

[4] Y. Yang, Q. Feng, Y. Sun, and Y. Dai, "Reputation trap: An powerful attack on reputation system of file sharing p2p environment," in *Proc. 4th Int. Conf. Security and Privacy in Communication Networks (SecureComm'08),* Istanbul, Turkey, Sept. 2008.

[5] A. Josang and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Electronic Commerce Conf.,* Bled, Slovenia, June 2002, pp. 324–337.

[6] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *Proc. 2nd ACM Conf. Electronic Commerce,* Minneapolis, MN, Oct. 2000.

[7] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via iterative refinement," in *Europhys. Lett.*, vol. 75, pp. 1006–1012, 2006.

[8] J. Zhang and R. Cohen, "A personalized approach to address unfair ratings in multiagent reputation systems," in *Proc. 5th Int. Joint Conf. Autonomous Agents and Multiagent Systems (AAMAS) Workshop on Trust in Agent Societies,* Hakodate, Japan, 2006, pp. 89–98.

[9] C. Sorrel. Apple expels 1,000 apps from store after developer scam. [Online]. Available: http://www.wired.com/gadgetlab/2009/12/apple-expels-1000-apps-from-store-after-developer-scam/

[10] W. Pan, N. Aharony, and A. Pentland, "Composite social network for predicting mobile apps installation," in *Proc. 25th Conf. Artificial Intelligence (AAAI-11),* San Francisco, CA, Aug. 2011.

[SP]

[standards **IN A NUTSHELL**] (continued from page 148)

Program (10047438, Development and International Standardization for MPEG Type-1 Standard Technology) funded by the Ministry of Trade, Industry, and Energy of Korea.

AUTHORS

Kiho Choi (aikiho@gmail.com) is a postdoctoral researcher at Hanyang University in Seoul, South Korea. He is the chair of the IVC Ad Hoc Group in MPEG.

Euee S. Jang (esjang@hanyang.ac.kr) is a professor at Hanyang University. He has been participating in MPEG in various leading roles since 1996.

REFERENCES

[1] ISO standards and patents [Online]. Available: http://www.iso.org/iso/standards_development/patents

[2] M. Hicks. (2007). JPEG hits new patent-infringement snag. [Online]. Available: http://www.eweek.com/c/a/Enterprise-Applications/JPEG-Hits-New-PatentInfringement-Snag/

[3] MPEG-LA official Web site. (2004). [Online]. Available: http://www.mpegla.com

[4] AT&T patent licensing Web site. [Online]. Available: http://www.att.com/gen/sites/ipsales?pid=19116

[5] I. Richardson, "Vcodex White Paper: Video compression patents," Vcodex Ltd., 2008, pp. 3–6.

[6] F. Mueller. (2012). Motorola calls $4 billion royalty figure "misleading" but doesn't dispute the number per se. [Online]. Available: http://www.fosspatents.com/2012/04/motorola-calls-4-billion-royalty-figure.html

[7] J. Bankoski, P. Wilkins, and Y. Xu, "Technical overview of VP8, An open source video codec for the Web," in *Proc. 2011 IEEE Int. Conf. Multimedia and Expo (ICME)*, pp. 1–6.

[8] H. Alvestrand and A. Grange, "VP8 as RTCWEB mandatory to implement." IETF, Internet-Draft/Informational draft–alvestrand–rtcweb–vp8-00, webrtc, Oct. 15, 2012.

[9] H. Alvestrand, A. Grange, J. Luther, M. Raad, and L. Bivolarski, "Google Inc.'s response to the CfP on Internet video technologies," ISO/IEC JTC1/SC 29/WG11/M29693, Vienna, Austria, July 2013.

[10] E. Protalinski. (2013). Google adds its free and open-source VP9 video codec to latest Chrome build. [Online]. Available: http://thenextweb.com/google/2013/07/01/google-adds-its-free-and-open-source-vp9-video-codec-to-latest-chrome-build/

[11] "Call for proposals (CfP) for Internet video coding technologies," ISO/IEC JTC1/SC29/WG11 N12204, 2011.

[12] R. Wang, Q. Yu, H. Lv, L. Chen, X. Zhang, S. Ma, T. Huang, and W. Gao, "IVC CE2: Internet Video Coding Test Model (ITM) performance improvements," ISO/IEC JTC1/SC 29/WG11/M29130, Incheon, South Korea, Apr. 2013.

[13] "Call for proposals (CfP) for Internet video coding technologies," ISO/IEC JTC1/SC29/WG11 N13546, 2013.

[14] "Resolutions of 105th meeting," ISO/IEC JTC1/SC29/WG11 N13648, 2013.

[15] "Resolutions of 104th meeting," ISO/IEC JTCø1/SC29/WG11 N13455, 2013.

[SP]