ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Mobile Social Networks to Support the Evaluation of a Service-Oriented Reliable Service

T. Sai Krishan
M.Tech Scholar,
Christu Jyoti Institute of Technology And Science
Colombonagar, Yeshwanthapur, Jangaon, Telangana

G.Rama Rao
Associate Professor
Christu Jyoti Institute of Technology And Science
Colombonagar, Yeshwanthapur, Jangaon, Telangana

ABSTRACT: ***In this paper, we propose a Trustworthy Service Evaluation (TSE) system to enable users to share service reviews in service-oriented mobile social networks (S-MSNs). Each service provider independently maintains a TSE for itself, which collects and stores users' reviews about its services without requiring any third trusted authority. The service reviews can then be made available to interested users in making wise service selection decisions. We identify three unique service review attacks, i.e., linkability, rejection, and modification attacks, and develop sophisticated security mechanisms for the TSE to deal with these attacks. Specifically, the basic TSE (bTSE) enables users to distributedly and cooperatively submit their reviews in an integrated chain form by using hierarchical and aggregate signature techniques. It restricts the service providers to reject, modify, or delete the reviews. Thus, the integrity and authenticity of reviews are improved. Further, we extend the bTSE to a Sybil-resisted TSE (SrTSE) to enable the detection of two typical sybil attacks. In the SrTSE, if a user generates multiple reviews toward a vendor in a predefined time slot with different pseudonyms, the real identity of that user will be revealed. Through security analysis and numerical results, we show that the bTSE and the SrTSE effectively resist the service review attacks and the SrTSE additionally detects the sybil attacks in an efficient manner. Through performance evaluation, we show that the bTSE achieves better performance in terms of submission rate and delay than a service review system that does not adopt user cooperation.***

Keywords: ***MSNs, Trustworthy service, Security.***

INTRODUCTION

SERVICE-ORIENTED mobile social networks (S-MSNs) are emerging social networking platforms over which one or more individuals are able to communicate with local service providers using handheld wireless communication devices such as smartphones. In the S-MSNs, service providers (restaurants and grocery stores) offer locationbased services to local users and aim to attract the users by employing various advertising approaches, for example, sending e-flyers to the nearby passengers via wireless connections.

Unlike the global counterparts, the interests of the local service providers are in serving the users in close geographic vicinity because most users choose services based on the comparison of the service quality and the distance advantage. In the S-MSNs, to establish the trust relations between the service providers and the users is particularly important. With a higher reputation, a service provider is more likely to be chosen by the users. However, the S-MSNs are autonomous and distributed networks where no third trusted authority exists for bootstrapping the trust relations. Therefore, for the users in the S-MSNs, how to enable the trust evaluation of the service providers is a challenging problem.

Trustworthy service evaluation (TSE) systems enable service providers or any third trusted authority to receive user feedback, known as service reviews or simply reviews, such as compliments and complaints about their services or products. By using the TSE, the service providers learn the service experiences of the users and are able to improve their service strategy in time. In addition, the collected reviews can be made available to

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the public, which enhances service advertising and assists the users in making wise service selections. The TSE is often maintained by a third trusted authority who is trusted to host authentic reviews. Popular TSE can be found in webbased social networks such as Facebook and online stores like eBay.

They are important marketing tools for service providers who target the global market. In this paper, we move the TSE into the S-MSN settings. We require service providers to maintain the TSE by themselves. In the meantime, we consider the users participate in the TSE in a cooperative manner. We will study possible malicious behaviors conducted by the service providers and the users. For ease of presentation, we refer to service providers as vendors in the sequel.

We consider an S-MSN composed of static vendors and mobile users that interconnect opportunistically. Each vendor is equipped with a wireless communication device that has a large storage space. In the TSE, the vendor stores and disseminates service information to the users. Note that the adoption of the TSE is subject to vendors' own decisions. However, the users expect to read comprehensive and authentic reviews of services, and this expectation makes vendors who support the TSE appear more attractive than the others.

Without in-network third trusted authorities in the SMSN, vendors are required to manage reviews for themselves. This requirement brings unique security problems to the review submission process. For example, vendors may reject or delete negative reviews and insert orged positive ones, and the malicious users can leave false negative reviews or drop the reviews from others to decrease the reputation of some particular vendors. In the design of the TSE for the S-MSN, security mechanisms must be included to resist these attacks. Notorious sybil attacks also cause huge damage to the effectiveness of the TSE.

RELATED WORK

Service-oriented mobile social networks (S-MSNs) are emerging social networking platforms over which one or more individuals are able to communicate with local service providers using handheld wireless communication devices such as smartphones. In the S-MSNs, service providers (restaurants and grocery stores) offer location-based services to local users and aim to attract the users by employing various advertising approaches, for example, sending e-flyers to the nearby passengers via wireless connections. Unlike the global counterparts, the interests of the local service providers are in serving the users in close geographic vicinity because most users choose services based on the comparison of the service quality and the distance advantage. In the S-MSNs, to establish the trust relations between the service providers and the users is particularly important. With a higher reputation, a service provider is more likely to be chosen by the users. However, the S-MSNs are autonomous and distributed networks In this paper, we move the TSE into the S-MSN settings. We require service providers to maintain the TSE by themselves. In the meantime, we consider the users participate in the TSE in a cooperative manner. We will study possible malicious behaviors conducted by the service providers and the users. For ease of presentation, we refer to service providers as vendors in the sequel. We consider an S-MSN composed of static vendors and mobile users that interconnect opportunistically. Each vendor is equipped with a wireless communication device that has a large storage space. In the TSE, the vendor stores and disseminates service information to the users. Note that the adoption of the TSE is subject to vendors' own decisions. However, the users expect to read comprehensive and authentic reviews of services, and this expectation makes vendors who support the TSE appear more attractive than the others.

SYSTEM PREMELIRIES

A. *ADMIN*

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such List all products, add categories, View categories, List users, List vendors, List user search history, list mobile users, Linkability attacker, List all Recommends, List all Reviews, Rejection & modification attackers and logout.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

B. ADD CATEGORIES

In this module, the admin can add n-number of product categories. If the admin want to add a new category, then admin will enter the product category name, then submit and that data will stored in data base. If admin want view to the newly added product category, then click on view categories button, it will display the category ID, category name and token.

C. LIST OF USERS

In this module, the Admin can view list of all users. Here all registered users are stored with the details such as user Image, User name, DOB, E-Mail, Mobile, Location and Secret Key.

D. LIST VENDORS

In this module, the Admin can view list of all Vendors. Here all registered venders are stored with the details such as vender Image, Vender name, E-Mail, Mobile, Address and Secret Key.

E. LIST USER SEARCHING HISTORY

This is controlled by admin; the admin can view the all user searching history. If admin clicks on list user search history button, then the server will display the all searching history with their tags such as user name, field searched, time & date for all the users.

F. LIST MOBILE USERS

In this module, the Admin can view list of all mobile users. Here all registered mobile users are stored with the details such as User name, Password, E-Mail.

G. LINKABILITY ATTACKERS

In this module, the admin can view the attacker details. If admin clicks on Linkability Attackers button, the admin will get attacker information with their tags such as Malicious User name, Product reviewed for, Date & Time, View user Details and View the product.

H. USER

In this module, there are n numbers of users are present. User should register before doing any operations. After registration successful he has to login by using authorized user name and password. After logged in he will do some operations such as view my details, search for products, View recommends, Request for user private key, request for token, Linkability Attckers and logout. If user clicks on my details button, then the server will give response to the user with their tags such as user Image, User name, DOB, E-mail, Mobile and Location. If more than one time review is made then that user is called as Linkability attack.

I. SEARCH FOR PRODUCTS

In this module, the user can search products. Before searching any product, the user should request private key, then admin will provide a private key. Then enter private key to search, enter category name search, it will display all related contents with their tags.

J. VENDOR

In this module, there are n numbers of vendors are present. Vendors should register before doing any operations. After registration successful he has to login by using authorized user name and password. After logged in he will do some operations such as view my details, Add products, View products, Linkability Attckers, request for Vendor access Key and logout. If Vendor clicks on my details button, then the server will give response to the user with their tags such as Vendor Image, Vender name, E-mail, Mobile and address.

K. ADD PRODUCTS

In this module, the vendor can add n-number of products. If the vendor wants to add a new product, then vendor will enter the private key provided by the admin and then enter product details like category, Product name, Product URL, Product description, Product uses and product image then submit, the product details will stored in the server.

L. ANDROID TEST BOOK

In this module, the user can install this application in his android mobile, after installation to use this application user should register with the valid information. After successful registration user should login by the valid user name and password. After logged

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

in user can perform operations like View users, View recommends and search product. User can search the products based on the categories. The admin can also use this application in the android phone; the admin should login by the valid user name and password. After logged in the admin will perform the some operations like view users, view all recommends, reject and modification attackers, linkability attackers, view vendors.

CONCLUSIONS

In this paper, we have proposed a TSE system for S-MSNs. The system engages hierarchical signature and aggregate signature techniques to transform independent reviews into structured review chains. This transformation involves distributed user cooperation, which improves review integrity and significantly reduces vendors' modification capability. We have presented three review attacks and shown that the bTSE can effectively resist the review attacks without relying on a third trusted authority. We have also considered the notorious sybil attacks and demonstrated that such attacks cause huge damage to the bTSE. We have subsequently modified the construction of pseudonyms and the corresponding secret keys in the bTSE, and obtained a SrTSE system. The SrTSE allows users to leave only one review toward a vendor in a predefined time slot. If multiple reviews with different pseudonyms from one user are generated, the real identity will be disclosed to the public. Security analysis and numerical results show the effectiveness of the SrTSE to resist the sybil attacks. Further trace-based simulation study demonstrates that the bTSE can achieve high SRs and low SDs.

REFERENCES

[1] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Proc. IEEE INFOCOM, pp. 1647-1655, 2011.

[2] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Seer: A Secure and Efficient Service Review System for Service-Oriented Mobile Social Networks," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 647-656, 2012.

[3] X. Liang, X. Li, T. Luan, R. Lu, X. Lin, and X. Shen, "Morality- Driven Data Forwarding with Privacy Preservation in Mobile Social Networks," IEEE Trans. Vehicular Technology, vol. 61, no. 7, pp. 3209-3222, Sept. 2012.

[4] T.H. Luan, L.X. Cai, J. Chen, X. Shen, and F. Bai, "VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution," Proc. IEEE CS Eighth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. Networks (SECON), pp. 359-367, 2011.

[5] J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS), pp. 251-260, 2002.

[6] J. Newsome, E. Shi, D.X. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 259-268, 2004.

[7] D. Quercia and S. Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proc. IEEE INFOCOM, pp. 336- 340, 2010.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A Dynamic Privacy- Preserving Key Management Scheme for Location-Based Services in VANETs," IEEE Trans. Intelligent Transportation Systems, vol. 13, no. 1, pp. 127-139, Mar. 2012.

[9] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.

[10] X. Boyen and B. Waters, "Full-Domain Subgroup Hiding and Constant-Size Group Signatures," Proc. 10th Int'l Conf. Practice and Theory Public Key Cryptography, pp. 1-15, 2007.

[11] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short Group Signature without Random Oracles," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS), pp. 69-82, 2007.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[12] C. Gentry and Z. Ramzan, "Identity-Based Aggregate Signatures," Proc. Int'l Conf. Public Key Cryptography, pp. 257-273, 2006.

[13] Y. Zhang, Z. Wu, and W. Trappe, "Adaptive Location-Oriented Content Delivery in Delay-Sensitive Pervasive Applications," IEEE Trans. Mobile Computing, vol. 10, no. 3, pp. 362-376, Mar. 2011.

[14] H. Tsai, T. Chen, and C. Chu, "Service Discovery in Mobile Ad Hoc Networks Based on Grid," IEEE Trans. Vehicular Technology, vol. 58, no. 3, pp. 1528-1545, Mar. 2009.

[15] Z. Zhu and G. Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System," IEEE Trans. Mobile Computing, vol. 12, no. 1, pp. 51-64, Jan. 2013.