Privacy Protection and Compromise Account Detection Social Media Network

S.M. Karpagavalli and M. Kanishma

Abstract--- Compromising social network accounts has become a profitable course of action for cyber criminals. By hijacking control of a popular media or business account, attackers can distribute their malicious messages or disseminate fake information to a large user base. The impacts of these incidents range from a tarnished reputation to multi-billion dollar monetary losses on financial markets. In our previous work, we demonstrated how we can detect large-scale compromises (i.e., so-called campaigns) of regular online social network users. In this work, we show how we can use similar techniques to identify compromises of individual high-profile accounts. High-profile accounts frequently have one characteristic that makes this detection reliable–they show consistent behaviour over time. We show that our system, were it deployed, would have been able to detect and prevent three real-world attacks against popular companies and news agencies. Furthermore, our system, in contrast to popular media, would not have fallen for a staged compromise instigated by a US restaurant chain for publicity reasons.

Keywords---Security, Online Social Network.

I. INTRODUCTION TO PROJECT

There is recent evidence that users very often negotiate collaboratively to achieve an agreement on privacy settings for co-owned information in Social Media. In particular, users are known to be generally open to accommodate other users' preferences, and they are willing to make some concessions to reach an agreement depending on the specific situation. However, current Social Media privacy controls solve this kind of situations by only applying the sharing preferences of the party that uploads the item, so users are forced to negotiate manually using other means such as e-mail, SMSs, phone calls, etc.- e.g., Alice and Bob may exchange some e-mails to discuss whether or not they actually share their they are willing to make some concessions to reach an agreement depending on the specific situation. However, current Social Media privacy controls solve this kind of situations by only applying the sharing preferences of the party that uploads the item, so users are forced to negotiate manually using other means such as e-mail, SMSs, phone calls, etc.- e.g., Alice andBob may exchange some e-mails to discuss whether or not they actually share their photo with Charlie. The problem with this is that negotiating manually all the conflicts that appear in the everyday life may be time-consuming because of the high number of possible shared items and the high number of possible assessors (or targets) to be considered by users; e.g., a single average user in Facebook has more than 140 friends and uploads more than 22 photos. Computational mechanisms that can automate the negotiation process have been identified as one of the biggest gaps in privacy management in social media.

The main challenge is to propose solutions that can be accepted most of the time by all the users involved in an item (e.g., all users depicted in a photo), so that users are forced to negotiate manually as little as possible, thus minimising the burden on the user to resolve multi-party privacy conflicts. Very recent related literature proposed mechanisms to resolve multi-party privacy conflicts in social media. Some of them need too much human intervention during the conflict resolution process, by requiring users to solve the conflicts manually or close to

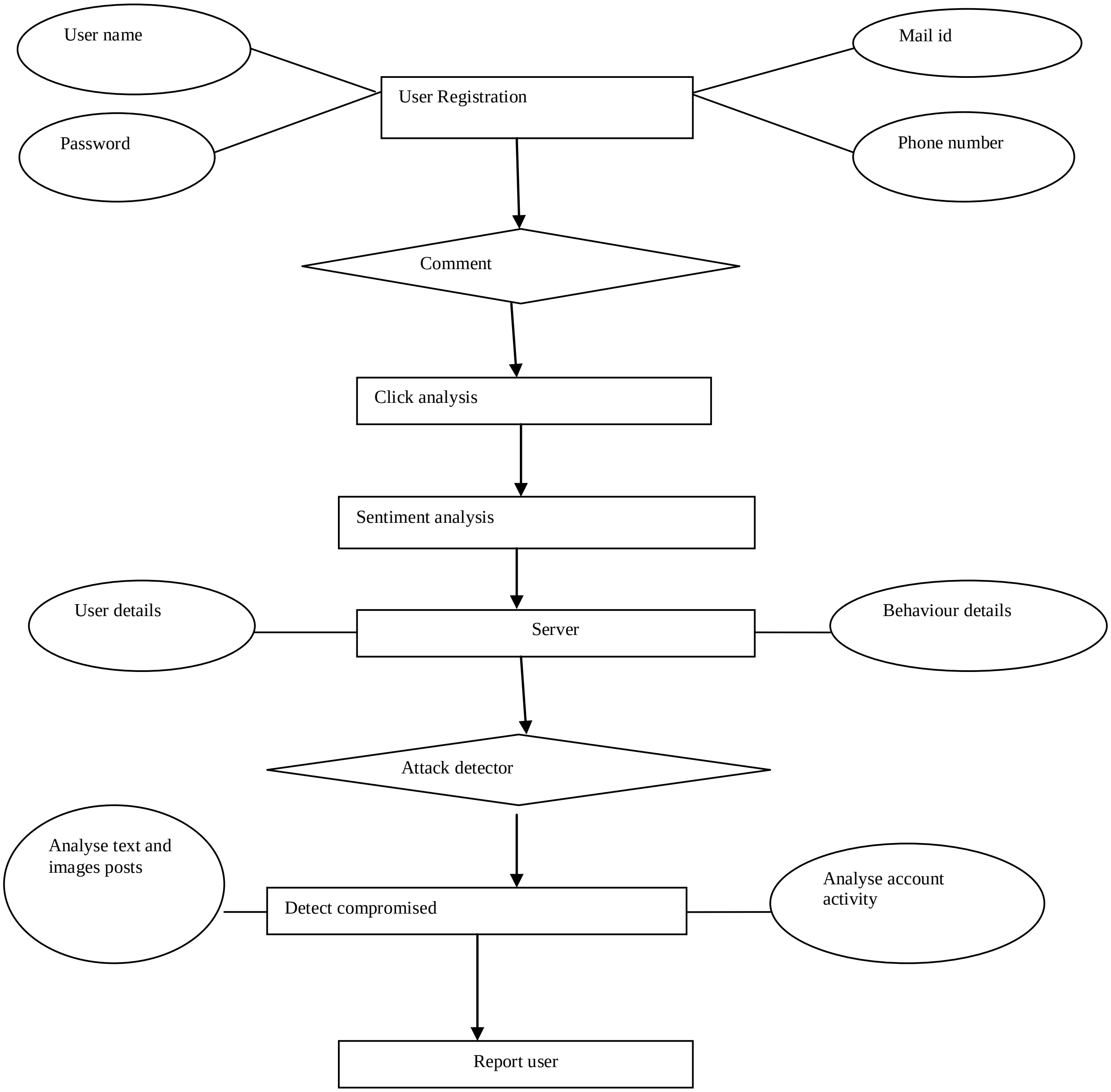
S.M. Karpagavalli, Associate. Prof, Al-Ameen Engineering College, Erode. E-mail:karpagam.rathan@gmail.com
M. Kanishma, M.E(CSE), Student, Al-Ameen Engineering College, Erode. E-mail:kanishmabe@gmail.com

manually; To this aim, the mediator estimates how willing each negotiating user may be to concede by considering: her individual privacy preferences, how sensitive the particular item is for her, and the relative importance of the conflicting target users for her.

II. SCOPE OF THE PROJECT

We conducted a user study comparing our mechanism to what users would do themselves in a number of situations. The results obtained suggest that our mechanism was able to match participants' concession behaviour significantly more often than other existing approaches. This has the potential to reduce the amount of manualuser interventions to achieve a satisfactory solution for all parties involved in multi-party privacy conflicts.We can provide security to user based on the location and time dependency in the future.

III. SYSTEM DESIGN



Existing System

- Very recent related literature proposed mechanisms to resolve multi-party privacy conflicts in social media.
- Some of them need too much human intervention during the conflict resolution process, by requiring users to solve the conflicts manually or close to manually; e.g., participating in difficult-to comprehend auctions for each and every co-owned item.
- Other approaches to resolve multi-party privacy conflicts are more automated, but they only consider one fixed way of aggregating user's privacy preferences (e.g., veto voting) without considering how users would actually achieve compromise and the concessions they might be willing to make to achieve it depending on the specific situation.
- Only considers more than one way of aggregating users' privacy preferences, but the user that uploads the item chooses the aggregation method to be applied, which becomes a unilateral decisionwithout considering the preferences of the others.

Disadvantage

- Computational mechanisms that can automate the negotiation process have been identified as one of the biggest gaps in privacy management in social media.
- The main challenge is to propose solutions that can be accepted most of the time by all the users involved in an item (e.g., all users depicted in a photo), so that users are forced to negotiate manually as little as possible, thus minimising the burden on the user to resolve multi-party privacy conflicts.

Proposed System

- In this paper, the system present the first computational mechanism for social media that, given the individual privacy preferences of each user involved in an item, is able to find and resolve conflicts by applying a different conflict resolution method based on the concessions users' may be willing to make in different situations.
- The mediator inspects the individual privacy policies of all users for the item and flags all the conflicts found. Basically, it looks at whether individual privacy policies suggest contradictory access control decisions for the same target user. If conflicts are found the item is not shared preventively.
- The mediator proposes a solution for each conflict found. To this aim, the mediator estimates how willing each negotiating user may be to concede by considering: her individual privacy preferences, how sensitive the particular item is for her, and the relative importance of the conflicting target users for her.

Advantage

- The use of a mediator that detects conflicts and suggests a possible solution to them.
- Works as an interface to the privacy controls of the underlying Social Media infrastructure
- The system also present a user study comparing our computational mechanism of conflict resolution and other previous approaches to what users would do themselves manually in a number of situations.
- The results obtained suggest our proposed mechanism significantly outperformed other previously proposed approaches in terms of the number of times it matched participants' behaviour in the study.

IV. STUDY OF THE SYSTEM

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

System Requirement Specifications

Hardware Requirements

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements

- Operating system: Windows 8.1.
- Coding Language: ASP.Net and C#.Net
- Database :SQLSERVER 2014

V. CONCLUSION

We present the first mechanism for detecting and resolving privacy conflicts in Social Media that is based on current empirical evidence about privacy negotiations and disclosure driving factors in Social Media and is able to adapt the conflict resolution strategy based on the particular situation. In a nutshell, the mediator firstly inspects the individual privacy policies of all users involved looking for possible conflicts. If conflicts are found, the mediator proposes a solution for each conflicts according to a set of concession rules that model how users would actually negotiate in this domain.

REFERENCES

[1] Y. Bachrach, M. Kosinski, T. Graepel, P. Kohli, and D. Stillwell, “Personality and patterns of Facebook usage”, Proceedings of the 4th Annual ACM Web Science Conference, Pp. 24-32, 2012.

[2] F. Benevenuto, T. Rodrigues, M. Cha and V. Almeida, “Characterizing user behaviour in online social networks”, Proceedings of the 9th ACM

SIGCOMM conference on Internet measurement conference, Pp. 49–62, 2009.

[3] Q. Cao, M. Sirivianos, X. Yang and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services”, Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, 2012.

[4] Detecting suspicious account activity. http://googleonlinesecurity. blogspot.com/2010/03/detecting-suspicious-account-activity.html.

[5] M. Egele, G. Stringhini, C. Kruegel and G. Vigna, “Compa: Detecting compromised accounts on social networks”, Symposium on Network and Distributed System Security, 2013.

[6] Face book tracks the location of logins for better security. http:// www.zdnet.com/blog/the system life/facebook-adds-better-security-tracks-the location-of-your-logins/2010.

[7] H. Gao, Y. Chenand K. Lee, “Towards online spam filtering in social networks”, Symposium on Network and Distributed System Security, 2012.

[8] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen and B.Y. Zhao, “Detecting and characterizing social spam campaigns”, Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, 2010.

[9] 250,000 twitter accounts hacked. http://www.cnn.com/2013/02/01/tech/social-media/twitter- hacked.

[10] 50,000 face book accounts hacked. http://www.ktsm.com/news/thousands-of-face book-accounts- hacked.