Browse Conferences > Information and Digital Techn...

< Previous | Back to Results | Next >

Detecting compromised accounts on the Pokec online social network

3 Author(s)

Jan Bohacik ; Antonin Fuchs ; Miroslav Benedikovic

View All Authors

Related Articles

Joint trajectory generation for redundant robots

Reconfiguration of resources in middleware

View All

Abstract | Authors | Figures | References | Citations | Keywords | Metrics | Media

Abstract:
Online social networks have billions of users worldwide when combined and they still keep increasing this amount. Their users typically develop trust relationships with the accounts of other users. But large numbers of users and potential gains from abuses of the trust relationships have attracted the attention of cyber-criminals. Therefore, it is important to stop accounts from being compromised by these criminals. In this paper, an anomaly model trained on the previous login data of users is applied to detection of compromised accounts. The login data comes from the Pokec online social network, which is the largest community in Slovakia where people can meet others and talk to their friends. The anomaly model watches sudden changes in the behavior of a user trying to log in to her or his account. A change in the behavior can indicate an attempt from someone else to compromise the account of the user. The efficiency of the anomaly model is validated with computation of measures such as sensitivity, specificity and overall accuracy. Achieved results are promising with a real potential to detect compromised accounts.

Published in: Information and Digital Technologies (IDT), 2017 International Conference on

Date of Conference: 5-7 July 2017

DOI: 10.1109/DT.2017.8024272

Date Added to IEEE *Xplore*: 04 September 2017

Publisher: IEEE

ISBN Information:
Electronic ISBN: 978-1-5090-5689-7
USB ISBN: 978-1-5090-5688-0
Print on Demand(PoD) ISBN: 978-1-5090-4689-8

Conference Location: Zilina, Slovakia, Slovakia

Keywords

IEEE Keywords
Social network services, Data models, Data mining, IP networks, Computational modeling, Mobile communication, Androids

Author Keywords
compromised account, anomaly model, login data, online social network

Authors

Jan Bohacik
University of Zilina, Data Mining Group, Pokec Team, Ringier Axel Springer Slovakia, Zilina, Slovakia

Antonin Fuchs
Data Mining Group, Pokec Team, Ringier Axel Springer Slovakia, Zilina, Slovakia

Miroslav Benedikovic
Department of Software Technologies, University of Pardubice, Pardubice, Czech Republic

Related Articles

Joint trajectory generation for redundant robots
T.C. Hsia; Z.Y. Guo

Reconfiguration of resources in middleware
H.A. Duran-Limon; G.S. Blair

Schedulability in model-based software development for distributed real-time systems
S.S. Yau; Xiaoyong Zhou

Configurable services for mobile users
A. Rasche; A. Polze

Distributed object-oriented real-time simulation of the multicast protocol RFRM
Y.S. Hong

Programming middle boxes with group event notification protocol
M. Smirnov

Wavelet-based lossy compression of barotropic turbulence simulation data
J.P. Wilson

Minimizing distortion via multiuser resource allocation
M. Mecking; T. Stockhammer

Implementation of a TMO-based real-time airplane landing simulator on a distributed computing environment
Min-Gu Lee; Sunggu Lee

Deriving interaction-prone scenarios in feature interaction filtering with use case maps
M. Nakamura; P. Leelaprute; T. Kikuno

Browse Conferences > Information and Digital Techn... < Previous | Back to Results | Next >

Detecting compromised accounts on the Pokec online social network

3 Author(s) Jan Bohacik ; Antonin Fuchs ; Miroslav Benedikovic View All Authors

Abstract Authors Figures References Citations Keywords Metrics Media

References

Citation Map

1. M. R. M. Aburrous, *Design and Development of an Intelligent Association Classification Mining Fuzzy Based Scheme for Phishing Website Detection with an Emphasis on E-Banking*, 2010.

2. Q. Cao, M. Sirivianos, X. Yang, T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services", *USENIX Conf. on Networked Systems Design and Implementation*, pp. 1-14, 2012.

3. M. Egele, G. Stringhini, C. Kruegel, G. Vigna, "COMPA: Detecting compromised accounts on social networks", *Network and Distributed System Security Symposium*, 2013.

< > View All

Contents

Online social networks are online platforms used by people to build social networks or social relations with those who share similar interests, activities, backgrounds or real-life connections [8]. They have become increasingly popular and time spent on the networks varies by country, but many countries average more than two hours per day per user [13]. People use them to share knowledge, opinions, and experiences; seek information and resources; and expand personal connections [14]. The most popular online social network in the world is Facebook with more than 1.8 billion active users [11]. Other popular networks include QZone with 632 million active users, Twitter with 317 million active users, LinkedIn with 106 million active users and VKontakte with 90 million active users. In Slovakia, the largest community where people can meet others and talk to their friends is the Pokec online social network. There are about 5.4 million people in Slovakia including children [10] and the network is visited daily by more than 400 thousand people. Overtime, the users of a social network build trust relationships with other people, friends, colleagues etc., which helps them to express their identity and gain social validation, find — people and communicate. Unfortunately, potential gains from abuses of these trust relationships have attracted the attention of cyber-criminals and their malicious activities. Information access and interaction is based on trust and users typically share a substantial amount of personal information with their friends [12]. Depending on the network, this information may be public or not. Some users also accept any friendship just to gain popularity and thus expose themselves to potential

users also accept any friendship just to gain popularity and thus expose themselves to potential attacks. There are also users who do not realize these risks even if they are well aware of e-mail spams for example.

Read document

Authors

References

1. M. R. M. Aburrous, *Design and Development of an Intelligent Association Classification Mining Fuzzy Based Scheme for Phishing Website Detection with an Emphasis on E-Banking*, 2010.
   Show Context

2. Q. Cao, M. Sirivianos, X. Yang, T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services", *USENIX Conf. on Networked Systems Design and Implementation*, pp. 1-14, 2012.
   Show Context

3. M. Egele, G. Stringhini, C. Kruegel, G. Vigna, "COMPA: Detecting compromised accounts on social networks", *Network and Distributed System Security Symposium*, 2013.
   Show Context

4. M. Egele, G. Stringhini, C. Kruegel, G. Vigna, "Towards detecting compromised accounts on social networks", *IEEE Transactions on Dependable and Secure Computing*, no. 99, 2015.
   Show Context

5. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, B. Y. Zhao, "Detecting and characterizing social spam campaigns", *ACM SIGCOMM Conference on Internet Measurement*, pp. 35-47, 2010.
   Show Context

6. J. Gosling, B. Joy, G. Steele, G. Bracha, A. Buckley, The Java Language Specification, USA:Oracle America, 2015.
   Show Context

7. R. C. Maheshwar, D. Haritha, "Survey on high performance analytics of bigdata with Apache Spark", *Int. Conf. on Advanced Communication Control and Computing Technologies*, pp. 721-725, 2016.
   Show Context View Article Full Text: PDF (343KB)

8. J. A. Obar, S. Wildman, "Social media definition and the governance challenge: An introduction to the special issue", *Telecommunications Policy*, vol. 39, no. 9, pp. 745-750, 2015.
   Show Context CrossRef Google Scholar

9. X. Ruan, Z. Wu, S. Jajodia, "Profiling online social behaviors for compromised account detection", *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 176-187, 2015.
   Show Context View Article Full Text: PDF (2379KB)

10. "Statistical Office of the Slovak Republic", *How Many of Us Are There What Households We Form*, pp. 14, 2015.
    Show Context

11. "The Stastistics Portal", *Most famous social network sites worldwide as of January 2017 rangked by number of active users (in millions)*, 2017, [online] Available: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
    Show Context

12. G. Stringhini, C. Kruegel, G. Vigna, "Detecting spammers on social networks", *Annual*

Computer Security Applications Conf., pp. 1-9, 2010.
Show Context Access at ACM

13. World Newsmedia Network Clobal Social Media Trends, UK:European Publishers Council, 2015.
Show Context

14. C. Xiao, D. M. Freeman, T. Hwa, "Detecting clusters of fake accounts in online social networks", *ACM Workshop on Artificial Intelligence and Security*, pp. 91-101, 2015.
Show Context Access at ACM

Keywords

Related Articles