Compromised user credentials detection in a digital enterprise using behavioral analytics

By: Shah, S (Shah, Saleh)[1]; Shah, B (Shah, Babar)[2]; Amin, A (Amin, Adnan)[1]; Al-Obeidat, F (Al-Obeidat, Feras)[2]; Chow, F (Chow, Francis)[3]; Moreira, FJL (Lopes Moreira, Fernando Joaquim)[4,5]; Anwar, S (Anwar, Sajid)[1]

Hide Web of Science ResearcherID and ORCID

Author	Web of Science ResearcherID	ORCID Number
Moreira, Fernando	P-9673-2016	http://orcid.org/0000-0002-0816-1445
Amin, Adnan	N-4652-2017	http://orcid.org/0000-0002-0852-8833

FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE
Volume: 93 **Pages:** 407-417
DOI: 10.1016/j.future.2018.09.064
Published: APR 2019
Document Type: Article
View Journal Impact

Abstract

In today's digital age, the digital transformation is necessary for almost every competitive enterprise in terms of having access to the best resources and ensuring customer satisfaction. However, due to such rewards, these enterprises are facing key concerns around the risk of next-generation data security or cybercrime which is continually increasing issue due to the digital transformation four essential pillars-cloud computing, big data analytics, social and mobile computing. Data transformation-driven enterprises should ready to handle this next-generation data security problem, in particular, the compromised user credential (CUC). When an intruder or cybercriminal develops trust relationships as a legitimate account holder and then gain privileged access to the system for misuse. Many state-of-the-art risk mitigation tools are being developed, such as encrypted and secure password policy, authentication, and authorization mechanism. However, the CUC has become more complex and increasingly critical to the digital transformation process of the enterprise's database by a cybercriminal, we propose a novel technique that effectively detects CUC at the enterprise-level. The proposed technique is learning from the user's behavior and builds a knowledge base system (KBS) which observe changes in the user's operational behavior. For that reason, a series of experiments were carried out on the dataset that collected from a sensitive database. All empirical results are validated through well-known evaluation measures, such as (i) accuracy, (ii) sensitivity, (iii) specificity, (iv) prudence accuracy, (v) precision, (vi) f-measure, and (vii) error rate. The experiments show that the proposed approach obtained weighted accuracy up to 99% and overall error of about 1%. The results clearly demonstrate that the proposed model efficiently can detect CUC which may keep an organization safe from major damage in data through cyber-attacks. (C) 2018 Published by Elsevier B.V.

Keywords

Author Keywords: Compromised user detection; Compromised activities detection; Knowledge-base system; Prudence analysis; Cluster-level pattern

Author Information

Reprint Address: Anwar, S (reprint author)

Inst Management Sci, Ctr Excellence Informat Technol, Peshawar 25000, Pakistan.

Addresses:

[1] Inst Management Sci, Ctr Excellence Informat Technol, Peshawar 25000, Pakistan

[2] Zayed Univ, Coll Technol Innovat, Abu Dhabi 144534, U Arab Emirates
Organization-Enhanced Name(s)
Zayed University

[3] Zayed Univ, Interdisciplinary Studies Dept, Abu Dhabi 144534, U Arab Emirates
Organization-Enhanced Name(s)
Zayed University

[4] Univ Portucalense, REMIT, IJP, Porto, Portugal
Organization-Enhanced Name(s)
Universidade Portucalense Infante D. Henrique

[5] Univ Aveiro, IEETA, Aveiro, Portugal
Organization-Enhanced Name(s)
Universidade de Aveiro

E-mail Addresses: hopeful021@gmail.com; babar.shah@zu.ac.ae; adnan.amin@imsciences.edu.pk; Feras.Al-Obeidat@zu.ac.ae; francis.chow@zu.ac.ae; fmoreira@upt.pt; sajid.anwar@imsciences.edu.pk

Publisher
ELSEVIER SCIENCE BV, PO BOX 211, 1000 AE AMSTERDAM, NETHERLANDS

Journal Information
Table of Contents: Current Contents Connect

Categories / Classification
Research Areas: Computer Science
Web of Science Categories: Computer Science, Theory & Methods

Document Information
Language: English
Accession Number: WOS:000459365800033
ISSN: 0167-739X
eISSN: 1872-7115

Other Information
IDS Number: HM3IA
Cited References in Web of Science Core Collection: 29
Times Cited in Web of Science Core Collection: 1

See fewer data fields

Cited References: 29

Showing 29 of 29 **View All in Cited References page** *(from Web of Science Core Collection)*

1. **A prudent based approach for compromised user credentials detection** **Times Cited: 3**
By: Amin, A.; Shah, B.; Anwar, S.; et al.
Cluster Comput Pages: 1-19 Published: 2017
[Show additional data]

2. **A prudent based approach for compromised user credentials detection** **Times Cited: 1**
By: Amin, A.; Shah, B.; Anwar, S.; et al.
Cluster Comput Published: 2017
[Show additional data]

3. Title: [not available] **Times Cited: 1**
By: Amin, Adnan.
Customer Churn Prediction in Telecommunication Sector using Rough Set Approach Volume: 4 Pages: 1-18 Published: 2016
Publisher: Neurocomputing, Press

4. **Compromised user credentials detection using temporal features: A prudent based approach** **Times Cited: 1**
By: Anwar, S.; Shah, B.; Khattak, A.M.; et al.
ACM International Conference Proceeding Series Published: 2017
Part F1278.

[Show additional data]

5. **Detecting Compromised Accounts on the Pokec Online Social Network** Times Cited: 1
By: Bohacik, Jan; Fuchs, Antonin; Benedikovic, Miroslav
2017 INTERNATIONAL CONFERENCE ON INFORMATION AND DIGITAL TECHNOLOGIES (IDT) Pages: 56-60 Published: 2017

6. **Detecting automation of twitter accounts: Are you a human, hot, or cyborg?** Times Cited: 1
By: Chu, Zi; Gianvecchio, S.; Wang, H.; et al.
IEEE Trans. Dependable Secure Comput Pages: 811-824 Published: 2010
[Show additional data]

7. Title: [not available] Times Cited: 2
By: Compton, P.; Preston, P.; Kang, B.
The Use of Simulated Experts in Evaluating Knowledge Acquisition Pages: 1-18 Published: 1995
Publisher: University of Calgary

8. **Entropy-based outlier detection using semi-supervised approach with few positive examples** Times Cited: 21
By: Daneshpazhouh, Armin; Sami, Ashkan
PATTERN RECOGNITION LETTERS Volume: 49 Pages: 77-84 Published: NOV 1 2014

9. **Social ties and their relevance to churn in mobile telecom networks** Times Cited: 50
By: Dasgupta, K.; Singh, R.; Viswanathan, B.; et al.
P 11 INT C EXT DAT T Pages: 668-677 Published: 2008
[Show additional data]

10. **Towards detecting compromised accounts on social networks** Times Cited: 3
By: Egele, M.; Stringhini, G.; Kruegel, C.; et al.
IEEE Trans. Dependable Secure Comput Published: 2015
[Show additional data]

11. **Compa: Detecting compromised accounts on social networks** Times Cited: 9
By: Egele, M; Stringhini, G; Kruegel, C; et al.
P NDSS Pages: 1-17 Published: 2013
[Show additional data]

12. **Outlier detection for temporal data: a survey** Times Cited: 11
By: Gupta, M; Gao, J; Aggarwal, CC; et al.
IEEE Trans. Knowl. Data Eng. Volume: 25 Pages: 1-20 Published: 2014
[Show additional data]

13. **A study of existing cross site scripting detection and prevention techniques in web applications** Times Cited: 2
By: Gupta, N.
Int. J. Eng. Comput. Sci. Volume: 3 Pages: 8445-8450 Published: 2014

14. Title: [not available] Times Cited: 930
By: Hawkins, D.
Identification of Outliers Published: 1980
Publisher: Chapman & Hall, London, U. K.

15. **The shape of digital transformation: A systematic literature review** Times Cited: 2
By: Henriette, E.; Feki, M.; Boughzala, I.
MED C INF SYST MCIS Pages: 14 Published: 2015
Retrieved from
URL: http://aisel.aisnet.org/mcis2015

16. **A survey of outlier detection methodologies** Times Cited: 1,020
By: Hodge, VJ; Austin, J
ARTIFICIAL INTELLIGENCE REVIEW Volume: 22 Issue: 2 Pages: 85-126 Published: OCT 2004

17. **An evaluation of statistical spam filtering techniques** Times Cited: 33
By: Le, Zhang; Zhu, Jingbo; Yao, Tianshun.
ACM Trans. Asian Lang. Inf. Process. Volume: 3 Issue: 4 Pages: 243-269 Published: December 2004

18. **Designing for digital transformation: Lessons for information systems research from the study of ICT and societal challenges** Times Cited: 29
By: Majchrzak, A.; Markus, M. L.; Wareham, J.
MIS Quarterly. Special Issue: ICT and Societal Challenge Volume: 40 Issue: 2 Pages: 267-277 Published: 2016

19. **Evaluating accuracy in prudence analysis for cyber security** Times Cited: 2
By: Maruatona, O.; Vamplew, P.; Dazeley, R.; et al.
Neural Information Processing. 24th International Conference, ICONIP 2017. Proceedings: LNCS 10638 Pages: 407-17 Part: pt.V Published: 2017

20. **DDoS Attacks With Randomized Traffic Innovation: Botnet Identification Challenges and Strategies** Times Cited: 7
By: Matta, Vincenzo; Di Mauro, Mario; Longo, Maurizio
IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY Volume: 12 Issue: 8 Pages: 1844-1859 Published: AUG 2017

21. **Interrater reliability: the kappa statistic** Times Cited: 1,298
By: McHugh, Mary L.
BIOCHEMIA MEDICA Volume: 22 Issue: 3 Pages: 276-282 Published: 2012

22. **Identifying Compromised Users in Shared Computing Infrastructures: a Data-Driven Bayesian Network Approach** Times Cited: 12
By: Pecchia, Antonio; Sharma, Aashish; Kalbarczyk, Zbigniew; et al.
2011 30TH IEEE INTERNATIONAL SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS (SRDS) Book Series: Symposium on Reliable Distributed Systems Proceedings Pages: 127-136 Published: 2011

23. **Profiling Online Social Behaviors for Compromised Account Detection** Times Cited: 18
By: Ruan, Xin; Wu, Zhenyu; Wang, Haining; et al.
IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY Volume: 11 Issue: 1 Pages: 176-187 Published: JAN 2016

24. **Outlier Detection: Applications and Techniques** Times Cited: 24
By: Singh, K.; Upadhyaya, S.
International Journal of Computer Science Issues Volume: 9 Issue: 1 Pages: 307 Published: 2012

25. **Consequences of connectivity: Characterizing account hijacking on twitter** Times Cited: 13
By: Thomas, K.; Li, F.; Grier, C.; et al.
P 2014 ACM SIGSAC C Pages: 489-500 Published: 2014
[Show additional data]

26. **Towards detecting anomalous user behavior in online social networks** Times Cited: 32
By: Viswanath, B; Bashir, MA; Crovella, M; et al.
P 23 USENIX SEC S US Pages: 223-38 Published: 2014
[Show additional data]

27. **Semi-supervised outlier detection based on fuzzy rough C-means clustering** Times Cited: 40
By: Xue, Zhenxia; Shang, Youlin; Feng, Aifen
MATHEMATICS AND COMPUTERS IN SIMULATION Volume: 80 Issue: 9 Pages: 1911-1921 Published: MAY 2010

28. Title: [not available] Times Cited: 1
By: Yang, Z.; Wilson, C.; Wang, X.; et al.
Uncovering Social Network Sybils in the Wild Volume: 8 Issue: 1 Published: 2011
[Show additional data]

29. **Outlier Detection Techniques for Wireless Sensor Networks: A Survey** Times Cited: 271
By: Zhang, Yang; Meratnia, Nirvana; Havinga, Paul

IEEE COMMUNICATIONS SURVEYS AND TUTORIALS Volume: 12 Issue: 2 Pages: 159-170 Published: 2010

Showing 29 of 29 **View All in Cited References page**