Accepted Manuscript

Title: Composition attack against social network data

Author: Jana Medkova

PII: S0167-4048(18)30005-1
DOI: https://doi.org/10.1016/j.cose.2018.01.002
Reference: COSE 1264

To appear in: *Computers & Security*

Received date: 25-5-2017
Revised date: 28-12-2017
Accepted date: 2-1-2018

Please cite this article as: Jana Medkova, Composition attack against social network data, *Computers & Security* (2018), https://doi.org/10.1016/j.cose.2018.01.002.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Composition attack against social network data

Jana Medkova[a]

[a]*Faculty of Informatics and Management, University of Hradec Kralove, Rokitanskeho 62, Hradec Kralove 50003, Czech Republic*

Jana Medková received her Bc. degree and Mgr. degree from Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic, in 2006 and 2009, respectively. She is currently a PhD. Student at Faculty of Informatics and Management, University of Hradec Králové. Her current research interests include data security and privacy, data analytics and personal data protection on the Internet. She also has interests in applied cryptography.

Highlights

- This paper deals with applying a composition attack to anonymized social network data.
- A new algorithm for the composition attack is proposed.
- Experiments on synthetic scale-free networks show the usability of the algorithm.
- The algorithm pairs rightly 20-30% from all appropriate nodes in the networks.

Abstract

The importance of social networks is growing with the fast development of social network technologies and the steady growth in their user communities. Given that the collection of data from social networks is essential for academic research and commercial applications, the prevention of leakage of sensitive information has become very crucial. The majority of anonymization techniques are focused on the threats associated with publishing one social network dataset. As most Internet users participate in more than one social network, a user's records are likely to appear in two published social network datasets. The level of anonymity of each dataset may present only a small security risk; however, there is no guarantee that a combination of the two datasets has the same level of anonymity. An attack on the privacy of an individual using two published datasets containing his/her records is called a composition attack. The composition attack was recently investigated as a threat to two relational datasets; however, it has not yet been considered as a potential danger to two datasets containing social network

Email address: jana.medkova@uhk.cz (Jana Medkova)

Download English Version:

https://daneshyari.com/en/article/6883968

Download Persian Version:

https://daneshyari.com/article/6883968

Daneshyari.com