Is pretty good, good enough? Social network analysis evaluates PGP data encryption

November 29 2023, by David Bradley

Credit: Pixabay/CC0 Public Domain

Research in the *International Journal of Business Information Systems* has used social network analysis to look at the most important and influential users utilizing PGP (pretty good privacy) data encryption to

reveal where there might be problems that could lead to compromise of data.

Victor Chang and Qianwen Ariel Xu of Teesside University, Middlesbrough U.K.; Lina Xiao of Xi'an Jiaotong-Liverpool University, Suzhou, China; Anastasija Nikiforova of the University of Latvia, Riga, Latvia; and Ben S.C. Liu of Quinnipiac University, Hamden, Connecticut, U.S., point out that PGP is most commonly used in protecting email but there is the issue of ensuring that the encryption keys being used have not been forged and so are not vulnerable to snooping or hacking by malicious third parties.

The team used social network analysis tools to examine the online interactions of PGP users with a view to identifying putative threats and vulnerabilities in the system. The team conducted two analyses: first a traditional centrality analysis and secondly the less common K-means clustering analysis. The former allowed them to identify the key figures within the network based on higher centrality, which suggests greater influence over other users. The latter, more precise method, allowed them to find clusters of important users in order to give them a comprehensive picture of the overall community structure of the network.

The team found that there were a range of interaction patterns among PGP users, ranging from frequent to isolated interactions. However, those users with higher centrality, tended to be more frequent PGP users, making them potential targets for scrutiny. The K-means clustering algorithm highlighted influential users who might be perceived as targets by malicious third parties. It also hinted at the converse, where a seemingly influential and trusted user may not be entirely legitimate and may themselves be present and gaining widespread trust for nefarious purposes, such as forging illicit PGP keys for fraudulent, espionage, and other dishonest activities.

The implications extend beyond PGP, offering a framework applicable to various domains such as business partnerships, supply chains, and criminal network studies.

More information: Victor Chang et al, The study of PGP web of trust based on social network analysis, *International Journal of Business Information Systems* (2023). DOI: 10.1504/IJBIS.2023.134956