A NOVEL APPROACH TO RECOGNIZE MALICIOUS APPLICATION IN FACE BOOK-FRAppE

Krishnaveni Shanmuga balu, T.Naga Raju

ABSTRACT

Our key commitment is in creating FRAppE seemingly the main apparatus concentrated on recognizing malicious applications on Facebook. To create FRAppE, we utilize data gathered by watching the posting conduct of 111K Facebook applications seen crosswise over 2.2 million clients on Facebook. In the first place, we recognize an arrangement of elements that help us recognize pernicious applications from considerate ones. For instance, we locate that malicious applications frequently share names with different applications, and they ordinarily ask for less consents than benign applications. Second, utilizing these recognizing highlights, we demonstrate that FRAppE can identify pernicious applications with 99.5% precision, with no false positives and a high genuine positive rate (95.9%). At long last, we investigate the biological system of pernicious Facebook applications and recognize instruments that these applications use to spread. Curiously, we locate that numerous applications connive and bolster each other; in our dataset, we find 1584 applications empowering the viral proliferation of 3723 different applications through their posts.

REFERENCES

http://thesocialskinny.com/100-social-media-statistics-for-2012/

Facebook, Palo Alto, CA, USA, “Facebook Opengraph API,” [Online]. Available:
http://developers.facebook.com/docs/reference/api/


Extracting facial feature is a key step in facial expression recognition (FER). Inaccurate feature extraction very often results in erroneous categorizing of facial expressions. Face preprocessing stage consists of face normalization and feature region localization steps to extract facial features efficiently. As regions of interest corresponding to relevant features are determined, Gabor jets are applied based on Gabor wavelet transformation to extract the facial points. Gabor jets are more invariable and reliable than gray-level values, which suffer from ambiguity as well as illumination variation while representing local features. Presentation on theme: "FRAppE: Detecting Malicious Facebook Applications" — Presentation transcript  15 FRAppE – Facebook’s Rigorous App Evaluator FRAppE Lite Based on Support Vector Machine Use features crawled on-demand No. of permissions required by an app Domain reputation of redirect URI Can be used user side FRAppE Addition of two aggregation based features: Similarity of app names Whether posted links are external Can be used only OSN side FRAppE Lite App ID Malicious.
ABOUT THE AUTHORS

Krishnaveni
Shanmuga balu

T.Naga Raja