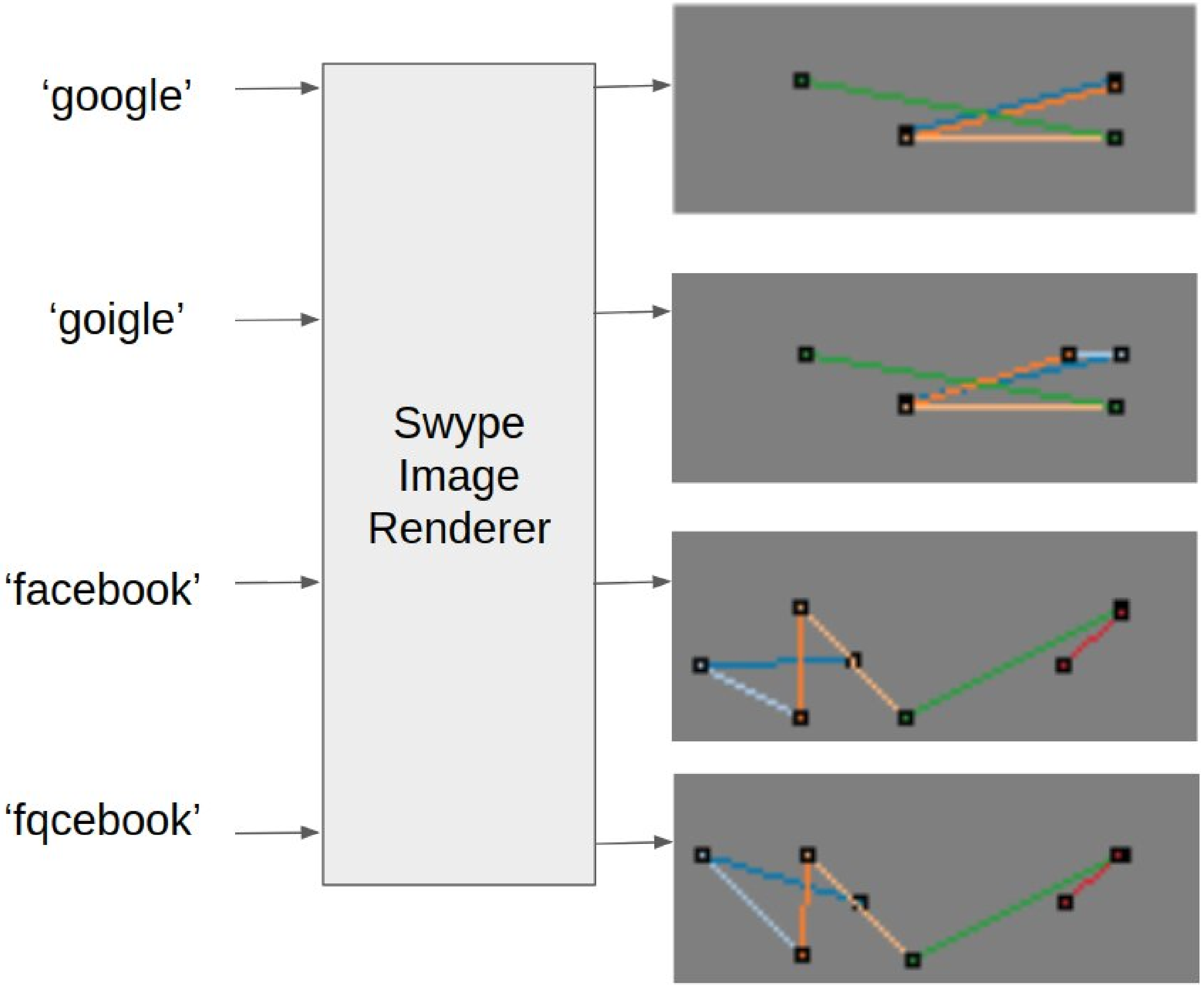
TechXplore

TypoSwype: An image recognition tool to detect typosquatting attacks

October 13 2022, by Ingrid Fadelli



Credit: Lee & Yam.

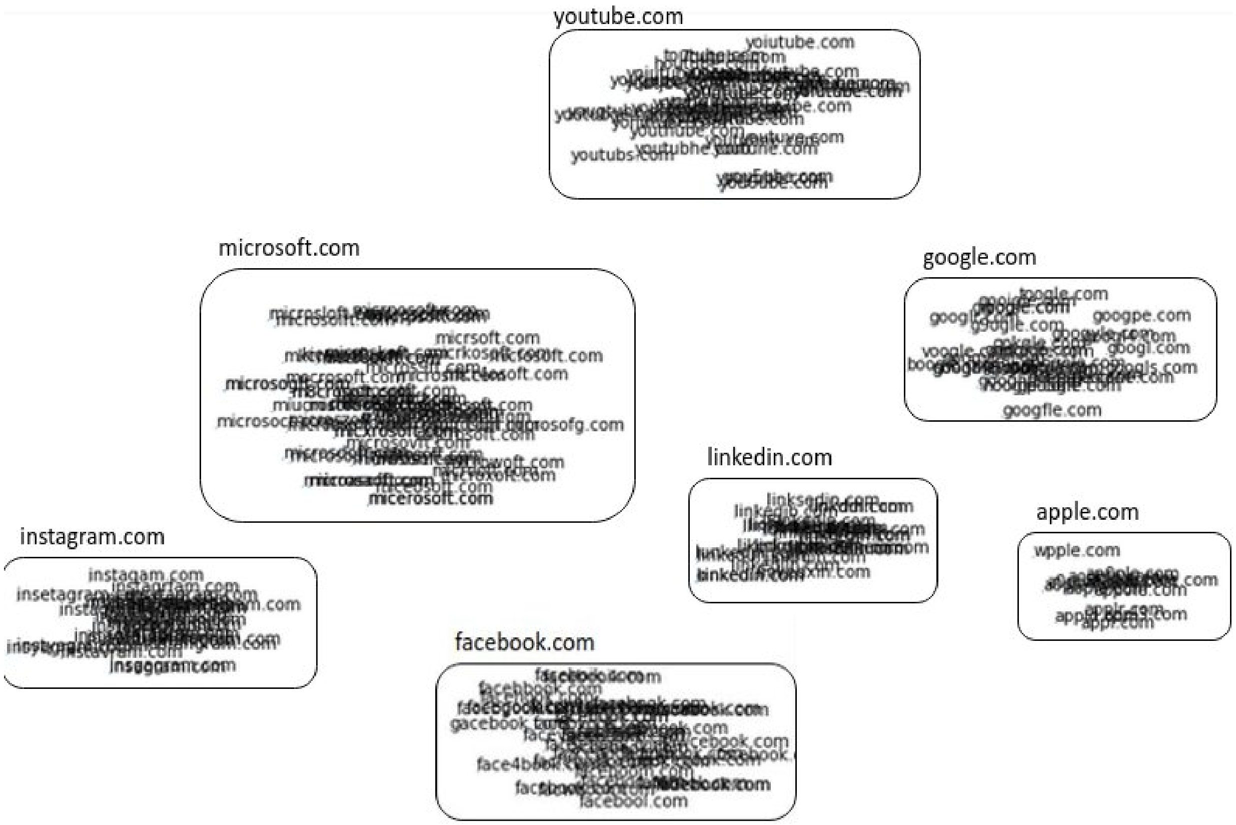
In recent decades, cyberattacks have become increasingly varied, introducing various strategies to lure users onto malicious websites or prompt them to share sensitive data. As a result, computer scientists are continuously trying to develop more advanced tools to detect and neutralize these attacks.

Typosquatting, one of the most common attacks carried out online, exploits the human tendency to misspell words when typing quickly or to misread words when they have small topographical errors. Typosquatting essentially consists in the creation of malicious websites with URLs that resemble established sites, but with slight typos (e.g., "fqcebook" instead of "facebook" or "yuube" instead of "youtube"). When a user mistakenly visits these websites, they might unwillingly download malware or end up sharing personal information with the attackers.

Most existing techniques for detecting these phishing attacks are based on spell-checking tools. While these tools can work in some instances, they do not generalize well, as their performance typically depends on the vocabulary of words used to train them.

Researchers at Ensign InfoSecurity, an end-to-end cybersecurity service provider based in Singapore, have recently created TypoSwype, an alternative tool for detecting typo-squatting attacks that is based on the analysis of images. This tool, introduced in a paper pre-published on arXiv, uses advanced image recognition techniques to convert strings into images that also consider the location of letters on the keyboard.

"Typosquatting makes use of typographical errors or typos (e.g. 'googgle.com' instead of 'google.com') to mislead users to access unwanted websites," David Yam, one of the researchers who carried out the study, told TechXplore. "Current techniques to tackle these phishing attacks utilize string edit distance which do not depend on the keyboard character positions ('g' is found in a different keyboard area from 'z') and hence are less accurate in catching typos (e.g. 'googgle.com' and 'googzle.com' is equally far apart from 'google.com'). We utilize image recognition techniques such as Convolutional Neural Networks (CNN) and specific loss functions to improve on typo-squatting detection."



Domains (left) and their Swype-like versions (right).typosquatted domains that have been clustered using their Swype-like versions. Credit: Lee & Peng David.

In contrast with other methods for detecting typosquatting introduced in the past, TypoSwype can capture the distance between different characters on the keyboard, by tracing lines between the buttons of consecutive characters on an imaginary keyboard. This helps to reduce errors that existing string edit distance metrics (i.e., methods that calculate how dissimilar two words or character sequences are from each other) are prone to making.

"We utilized image recognition techniques because it can batch process multiple possible typosquatted domains at one shot, enabling faster processing as compared to string matching solutions," Lee explained. "Also, utilizing Swype inputs allows us to visually inputs which are likely to be typosquats of each other, such as 'fqcebook' and 'facebook.'"

Yam and his colleague Lee Joon Sern evaluated their typosquatting detection tool in a series of tests, comparing its performance with that of the DLD algorithm, a widely used cybersecurity model. They found that TypoSwype could detect typosquatting more reliably than DLD, while also accurately identifying the well-established and safe domains that attackers were trying to copy or "typo-squat."

"TypoSwype is (to the best of our knowledge) the first application of CNNs to tackling typosquatting using Swype inputs," Yam said. "Using Swype inherently captures the keyboard distance metric that typographical errors usually have. We also use of Triplet loss and NT-Xent loss as superior mechanisms to train our model because it provides a minimum boundary between non-similar Swype images. This enables us to improve metrics (F1 score) in detecting typosquatting domains that are already fairly similar (1 edit distance away) by string edit distance matching algorithms."

The recent work by this team of researchers could soon inspire the development of other cybersecurity techniques based on image recognition models. Meanwhile, TypoSwype will be included within Ensign InfoSecurity's suite of phishing detection tools, making it available to users worldwide.

More information: Joon Sern Lee, Yam Gui Peng David, TypoSwype:

An imaging approach to detect typo-squatting. arXiv:2209.00783v1 [cs.CR], arxiv.org/abs/2209.00783

© 2022 Science X Network

Citation: TypoSwype: An image recognition tool to detect typosquatting attacks (2022, October 13) retrieved 26 April 2024 from https://techxplore.com/news/2022-10-typoswype-image-recognition-tool-typosquatting.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.