Contribution ID: **15** Type: **Paper presentation**

Malicious Short URLs Detection Technique

Friday 22 September 2023 10:00 (20 minutes)

Nowadays, as the smartphone's performance grew a lot, being comparable with the one of computer systems, people are more attracted due to their capabilities and tend to use them in almost all activities. This fact determined the attackers to also consider the mobile devices among their targeted platforms. The easiest way for adversaries to get access to a smartphone is via SMS phishing (smishing), where they try to lure the victims into accessing a malicious URL to provide confidential data or download malware. To hide the features of these URLs and to avoid the text messaging's length restrictions, attackers use URL shortening services. In this paper, we propose an exhaustive system to detect malicious short URLs in smishing attacks by leveraging threat intelligence data from popular platforms like VirusTotal, and PhishTank, and by employing various Machine Learning (ML) algorithms that classify the SMS based on the features of the final redirected URL. Our system works for every URL, no matter the shortening service used either public or custom. Moreover, concerning the ML classifier, we took a publicly available balanced dataset for training, improved its feature set, and obtained an accuracy of approximately 97\%. The dataset contains 90 features that belong to three categories: the URL's lexical properties, external specifications, and the website content. We have tested our proposed ML model against JRip, PART, J48, and Random Forest algorithms, the last one being the most accurate. To showcase the effectiveness of our solution, we have implemented an Android app from scratch that detects malicious short URLs in SMS messages and notify the user concerning their legitimacy.

Author: Mr STOLERIU, Răzvan (University Politehnica of Bucharest)

Co-authors: Dr MOCANU, Bogdan-Costel (University Politehnica of Bucharest); Dr NEGRU, Cătălin (University Politehnica of Bucharest); POP, Florin (University Politehnica of Bucharest, Romania / National Institute for Research & Development in Informatics –ICI Bucharest, Romania)

Presenter: Mr STOLERIU, Răzvan (University Politehnica of Bucharest)

Session Classification: Session C

Track Classification: Security & Resilience in Cyber-Physical Systems