Contribution ID: **4** Type: **Abstract for Research Paper**

A NOVEL APPROACH FOR DETECTING AND PREVENTING THE WI-FI EVIL TWIN ATTACK

Wi-Fi connectivity affords users unmatched convenience when it comes to accessing computer networks. However, this convenience comes at a huge security cost – Wi-Fi has been plagued by various security challenges that continue to expose users to a potential loss of the confidentiality, integrity and availability of their data. One of these challenges is the evil twin attack – an attack that involves creating a duplicate access point and redirecting users to connect to it. In a successful attack, the victim will unknowingly transmit all their communications through the attacker's equipment, thereby risking interception. The ease of setting up such a rogue access point and the difficulty in detecting one pose a serious threat to the privacy and data security of both organizations and individuals who rely on Wi-Fi connectivity for their day-to-day needs. Substantial research has gone into finding a solution to this problem, but none of the proposed solutions seems to be effective as the attack remains prevalent and effective to date. It is against this background that this paper seeks to describe a novel approach for detecting and preventing the Wi-Fi evil twin attack. The main objective of the study is to identify an approach that can effectively detect a rogue access point and prevent unsuspecting users from connecting to it. Study methods used in the research includes systematic literature review and design science, while the theory of General Deterrence provides its theoretical underpinning.

Primary author: KENGOCHA, clifford (kabarak university)

Track Classification: Information Security