User-side Evil Twin Attack Detection Using Time-Delay Statistics of TCP Connection Termination

En-Chun KUO, Ming-Sang CHANG, Da-Yu KAO*
Department of Information Management, Central Police University, Taoyuan City 333, Taiwan
im831216@mail.cpu.edu.tw, mschang@mail.cpu.edu.tw, camel@mail.cpu.edu.tw

***Abstract*—Open wireless network services are now freely shared in the most of the public areas but have barely protection about communication data between the web server and the client-side. Evil Twin Attack (ETA) appears to be a legitimate Wi-Fi Access Point (AP) and becomes a common attack in smart home environments where attackers can compromise the security of the connected devices. By setting up a rogue access point, deceiving users into establishing the network connection with the same SSID as the legitimate one, the attacker can launch the man- in-the-middle attack and steal some private information. To identify the fake APs, this paper presents an improved and practical client-side detection method to mathematically detect the ETA by observing the time-delay of TCP connection termination between the client and the server. This proposed time-delay model is further experimented and measured from the following three date-time intervals: Initial Ending, Ending Response, and Confirmed Ending. The utility of this model is illustrated by applying it to the client side which makes it more convenient for users to deploy and ensure their security with high detection rate.**

***Keyword*—Access Point, Wi-Fi Network, Evil Twin Attack, TCP Connection Termination, Time-Delay Analysis**

En-Chun Kuo is a student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan

Ming-Sang Chang is a Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. His academic research interests include broadband network, performance analysis, and network planning.

Da-Yu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. With a Master degree in Information Management and a Ph.D. degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.