

BYOD for UAE University

Sajid Ali

The current UAEU Wireless WPA2-Enterprise has some powerful built-in security features. However, it is still vulnerable to attacks, which presents a number of challenges the IT team takes seriously.

Challenge # 1: Device Variation

Support of 802.1x is inconsistent across devices, even within the same OS, and each device has unique characteristics that can make them behave unpredictably.

Challenge # 2: MITM (Man-in-the-Middle) Attack

The existing WPA2 Enterprise forces users to only connect to the more secure UAEU Official Wireless SSID (UAEU-SkyNet). However, a secure

connection is meaningless if any honeypot or imposter signal is in place. We do detect rogue access points, including Man-in-the-Middle attacks, but users can still be vulnerable. A person with a laptop can quietly gather user credentials wherever devices might pass through and try to auto-connect.

Challenge # 3: Password Change Problem

UAEU have set up password expire policy on a regular basis face additional burden with WPA2-Enterprise. Password expired user lose wireless connectivity until reconfigured.

