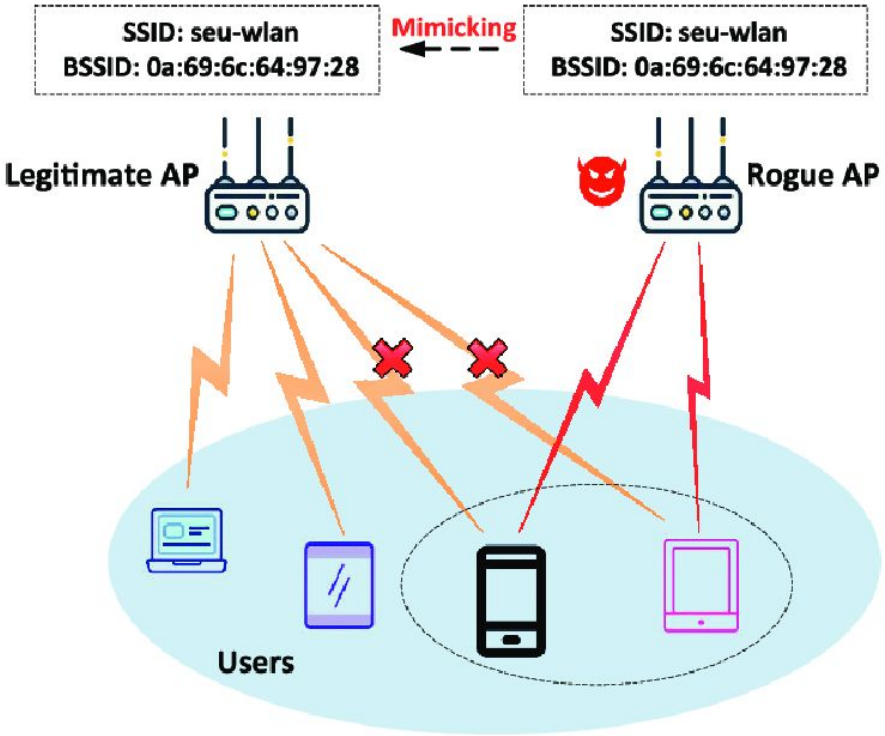
An approach to detect evil twin attack (Rogue AP Attack)

Presented by:
Florian KAMSU KOM

Under the supervision of
Gérard CHALHOUB, Maxime PUYS

How does Rogue AP attack work?



Why Rogue AP attack?

- Hard to detect
- Garner reported that nearly 20 % of organizations have rogue access points inside their premise.

Existing approach

- Consider that an AP has a fixed position, then measure the received signal strength on many distances, store it in a database. Compare the received signal to the database when a device wants to connect to an AP.
- Based on the fact that a signal transmit by an AP is unique due to “micro difference” between hardware of APs.

Work plan

- Modeling a scenario of attack also the complexity of the environment by using a simulator (NS3).
- Use of machine learning to recognize legitimate AP by extracting some features from the signal of the AP.

Thanks for your attention