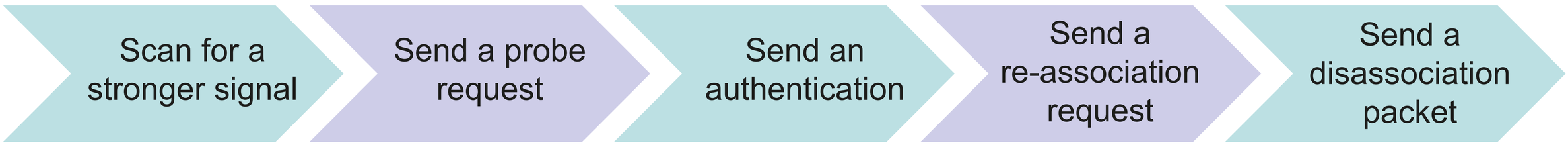
A Roaming Attack to Wireless LAN

Student: Lau Kar Yee **Programme: BEng4CE** **Supervisor: Dr K H Yeung**

Background

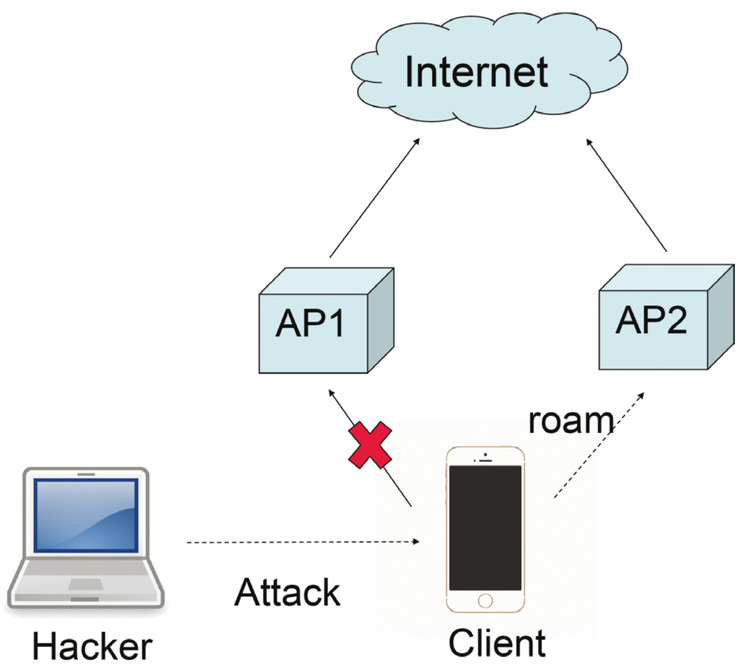
- Roaming networks are commonly used in the campuses and workspaces, to serve a huge amount of users
- Occurs when a client device moves from place to place
- Done seamlessly, the client would not notice the processes

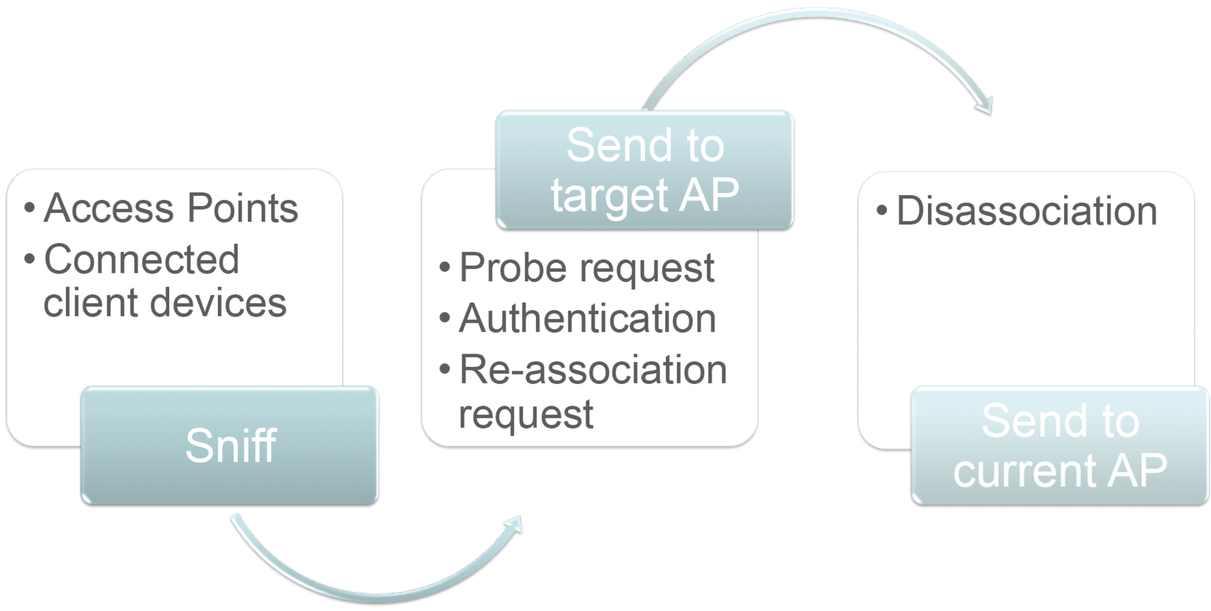


- Aims to discover the loophole in the roaming networks and perform an attack

Methodology

- Build a Python program to roam a client device manually
- Sniff the MAC address of the APs and the client devices
- Perform the roaming attack by using the client's MAC address





Results

- Client would be forced to roam from AP1 to AP2
- The client would not notice :
  - The processes of the roaming attack
  - Who implemented the attack

Applications

- Roaming different clients to the targeted AP to overload the traffic
- Performing roaming attack to attack a client in a long distance

CityU
香港城市大學
City University of Hong Kong
專業 創新 胸懷全球
Professional·Creative
For The World