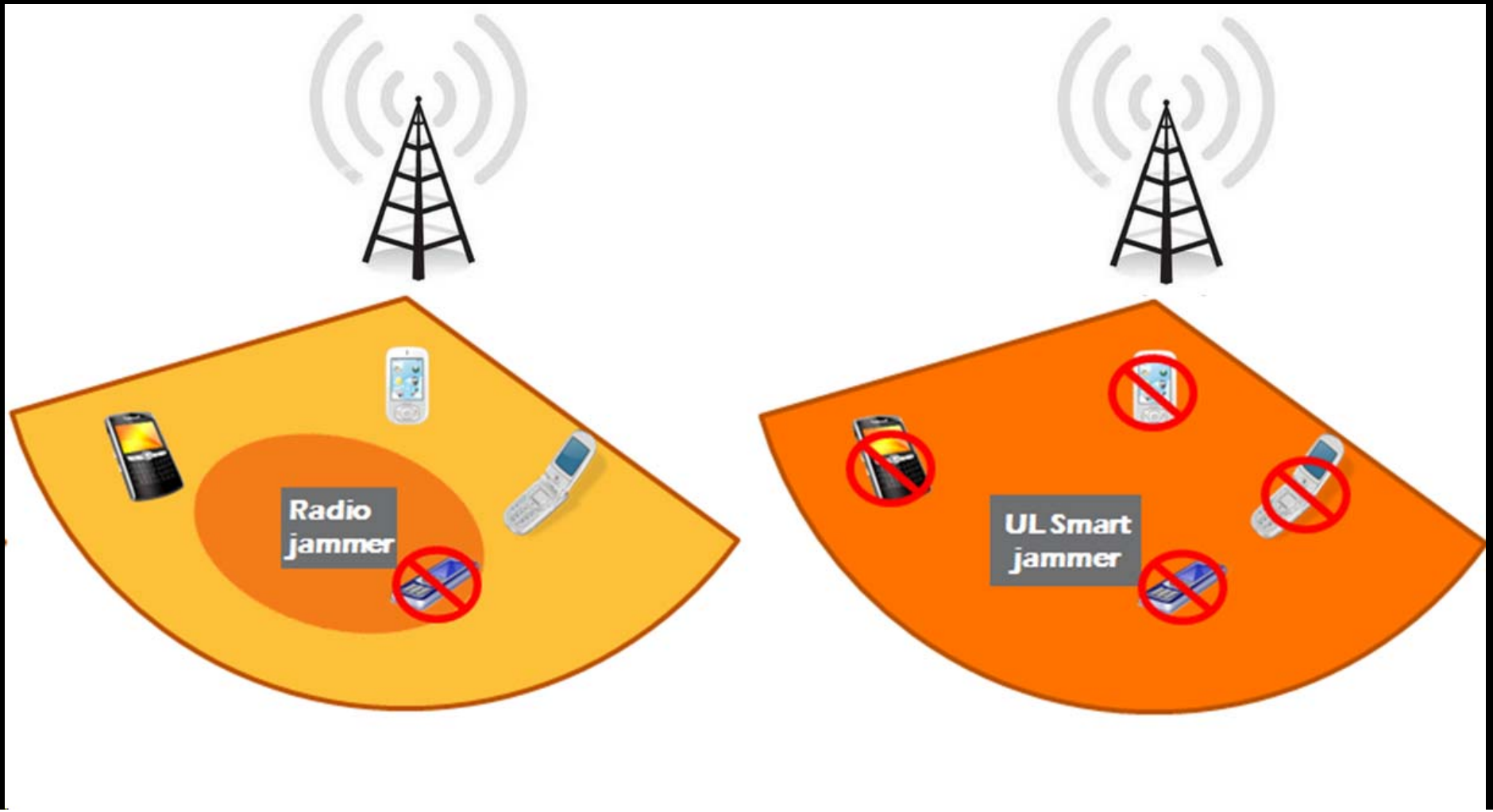
行動偽基站的安全疑慮與演示

TTC Su C C 2017/10/14

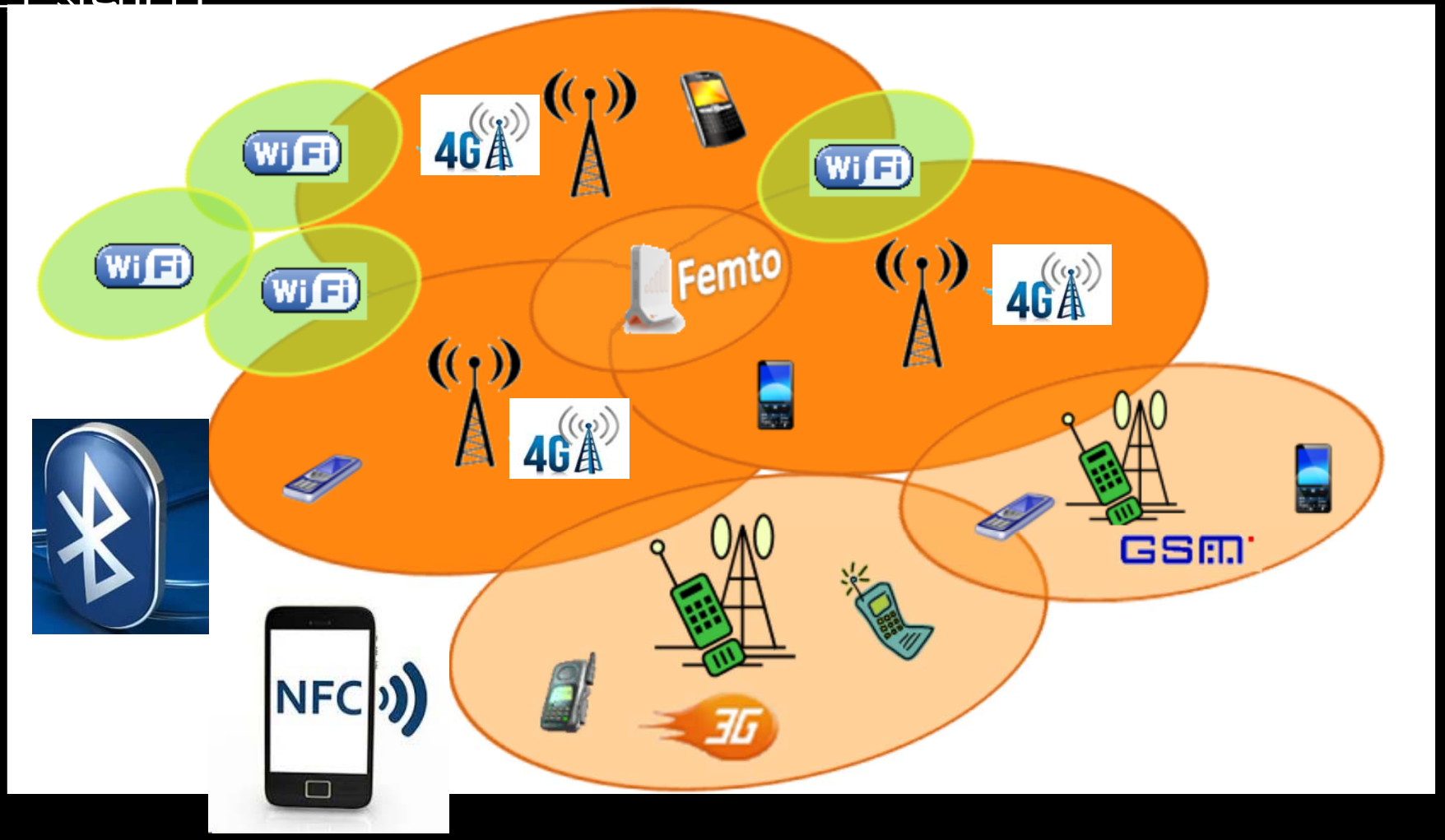
LTE空中介面漏洞

- 空中介面的干擾：OFDMA調變下利用高訊號準位，覆蓋在原本的LTE訊號上面，進行阻斷式干擾。
- 異質網路：同時具有WiFi、LTE、Bluetooth、NFC等無線接取引發漏洞。
- LTE系統本身安全性漏洞。

空中介面的干擾



異質網路

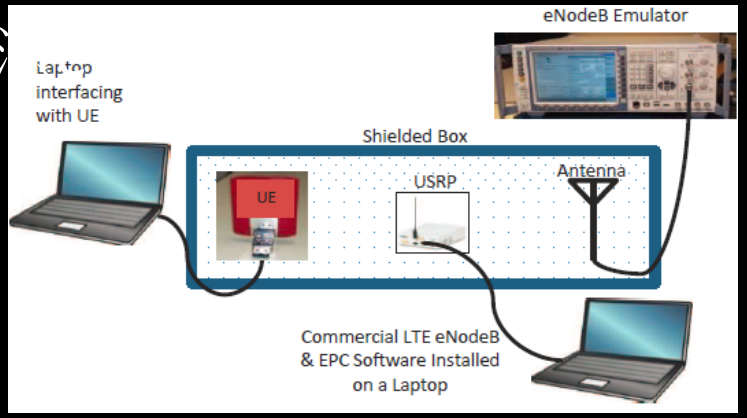


LTE系統本身漏洞

- Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing
  - 2015 IEEE CSCN Conference\Mina Labib, Vuk Marojevic, and Jeffrey H. Reed, Virginia Tech ,USA

測試架構

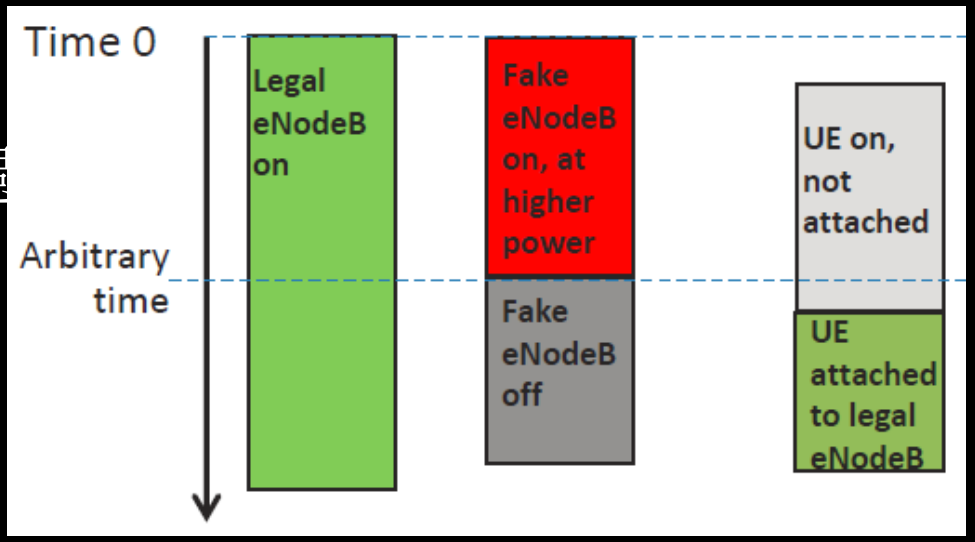
- R&S CMW500 ：模擬合法的eNB
- EPC 軟體(3GPP R12)+ USRP：模擬分
- UE(LTE USB dongle)+SIM卡：模擬UE
- RF屏蔽盒和天線



Test Case 1

	Fake eNodeB	Legal eNodeB
Physical Cell ID	1	2
Cell ID	0x01A2D001	0x01A2D000
Authentication Key	Invalid	Valid
Power	Higher	Lower

1. 假的eNB發射High power
2. 開啟合法的eNB
3. 開啟UE，觀察UE在cell 選擇的過
4. 在任意時間點切斷假的eNB

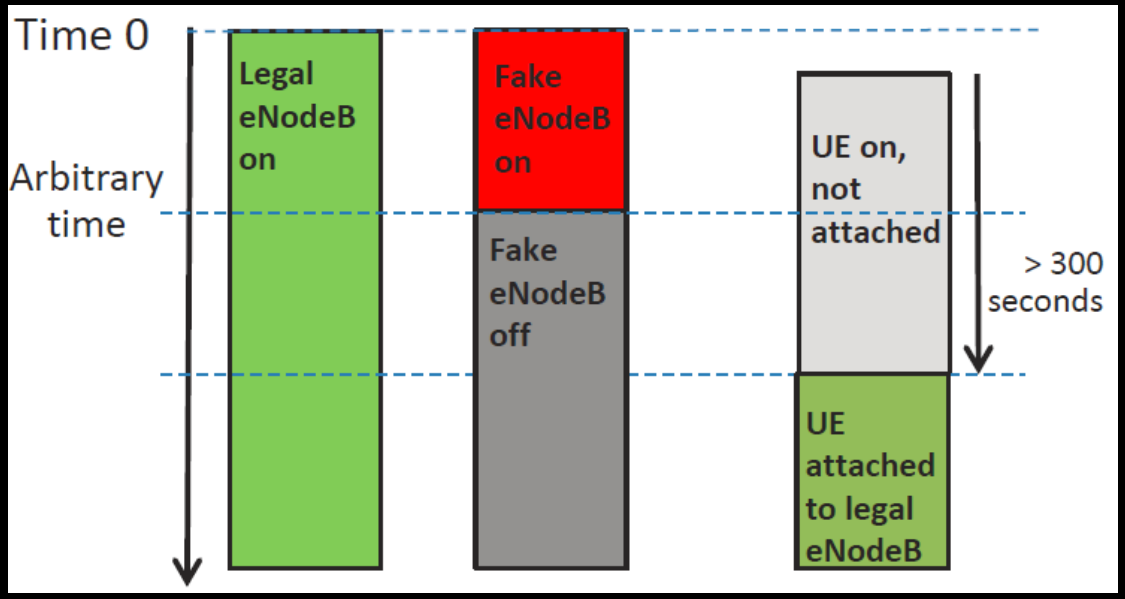


- 當假的eNB發射時，會產生蓋台。
- UE會把這個cell當作錯誤或禁止

Test Case 2

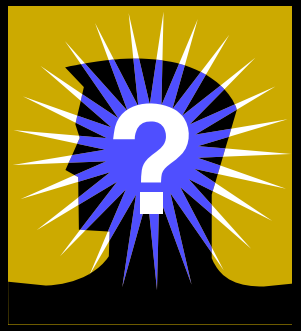
- 假的與真的eNB，使用相同PCI
- UE不能登錄到假的eNB
- 等假的eNB關閉後，也回不去了

	Fake eNodeB	Legal eNodeB
Physical Cell ID	1	1
Cell ID	0x01A2D001	0x01A2D000
Authentication Key	Invalid	Valid
Power	Higher	Lower
cellBarred	True	False



觀賞影片

Questions?



強力徵求
有理想抱負的你加入TTC

職 缺 介紹

資訊安全工程師:

- 參與資通安全中心（SOC、ISAC、CERT）架構規劃與建置。
- 協助分析、處理資安事件，並提出處置措施。
- 進行惡意程式或郵件之檢測，挖掘安全性漏洞與威脅。
- 資訊安全設備自動化程式撰寫、測試、佈署。
- 撰寫資訊安全技術相關計劃書、研究報告。
- 團隊及協同合作，以專案管理方式進行系統導入。
- 資訊安全設備:防火牆、入侵偵測、弱點掃描系統維護。
- 網站、IP網路維護、SPLUNK系統使用。

工作地點: 路竹/板橋