WLAN Security Demo

Sang Young
wsyoung@wsyoung.com
PISA & WTIA
Date: 2010.03.27

Disclaimer

This material is to provide information on WiFi security risks and mitigation measure. It should not be used for malicious intent. Unauthorized Access to computer system is an offense.

The points made here are kept concise for the purpose of presentation. If you require details of test and implementation please refer to technical references.

WEP Cracking Latest Update

蹭網片

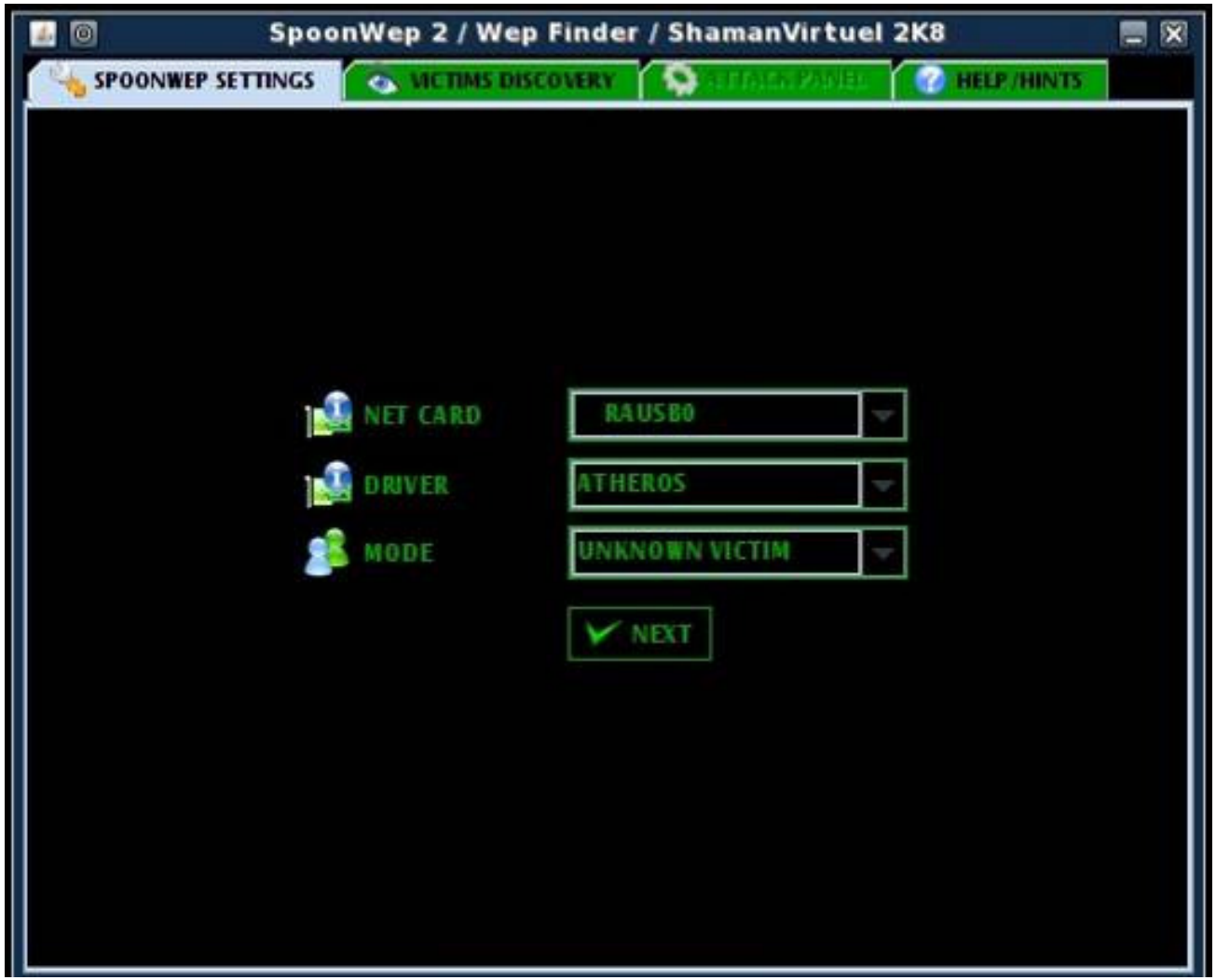
- 蹭
  - 粵音: sang3
  - 解說: 白佔便宜

http://tool.httpcn.com/Html/Zi/37/KOTBILTBCQXVETBD.shtml

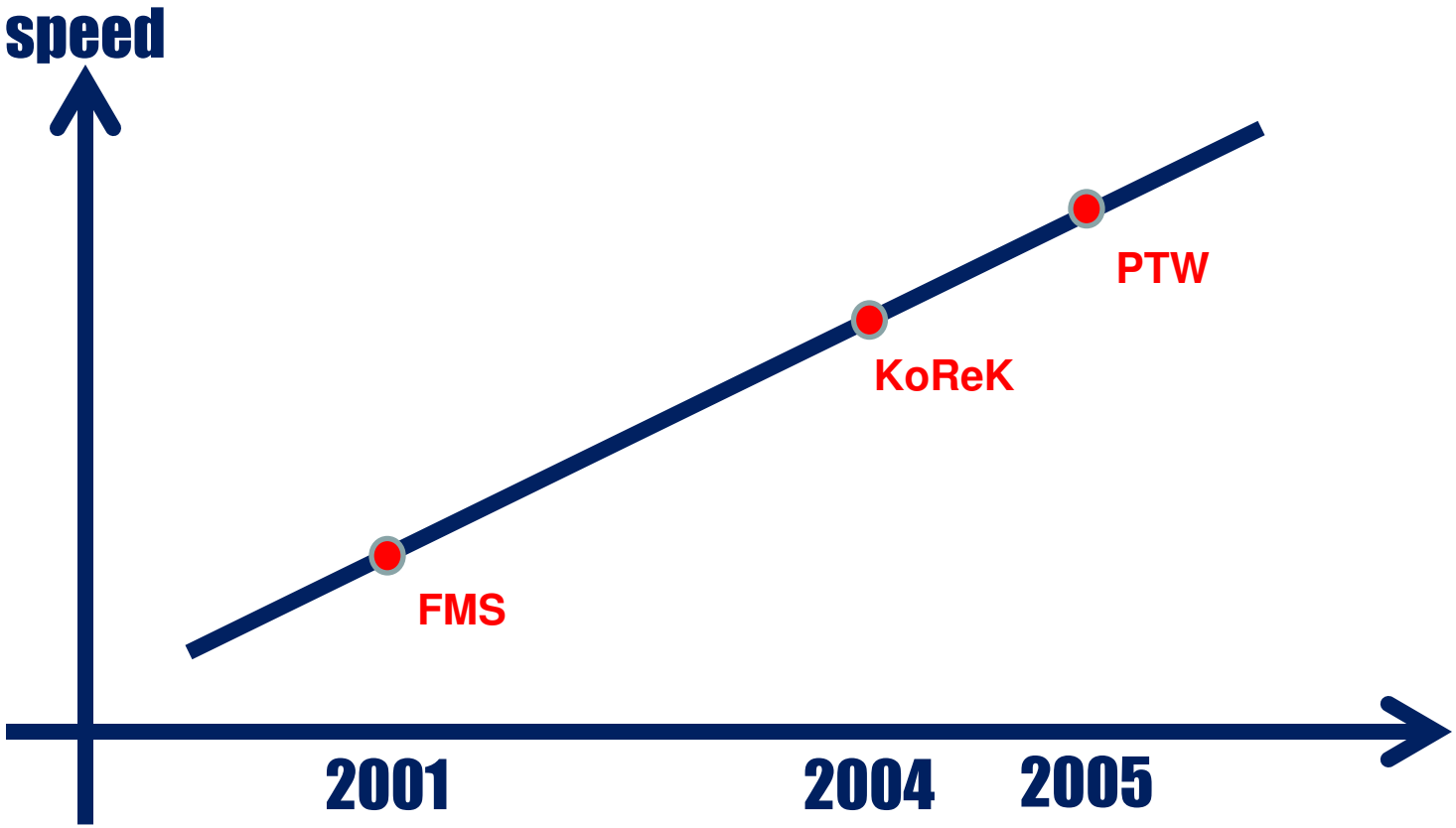
蹭網卡

- 蹭網卡：用作白佔無線網絡便宜的工具
  - USB無線網絡卡
  - Software for WEP Cracking

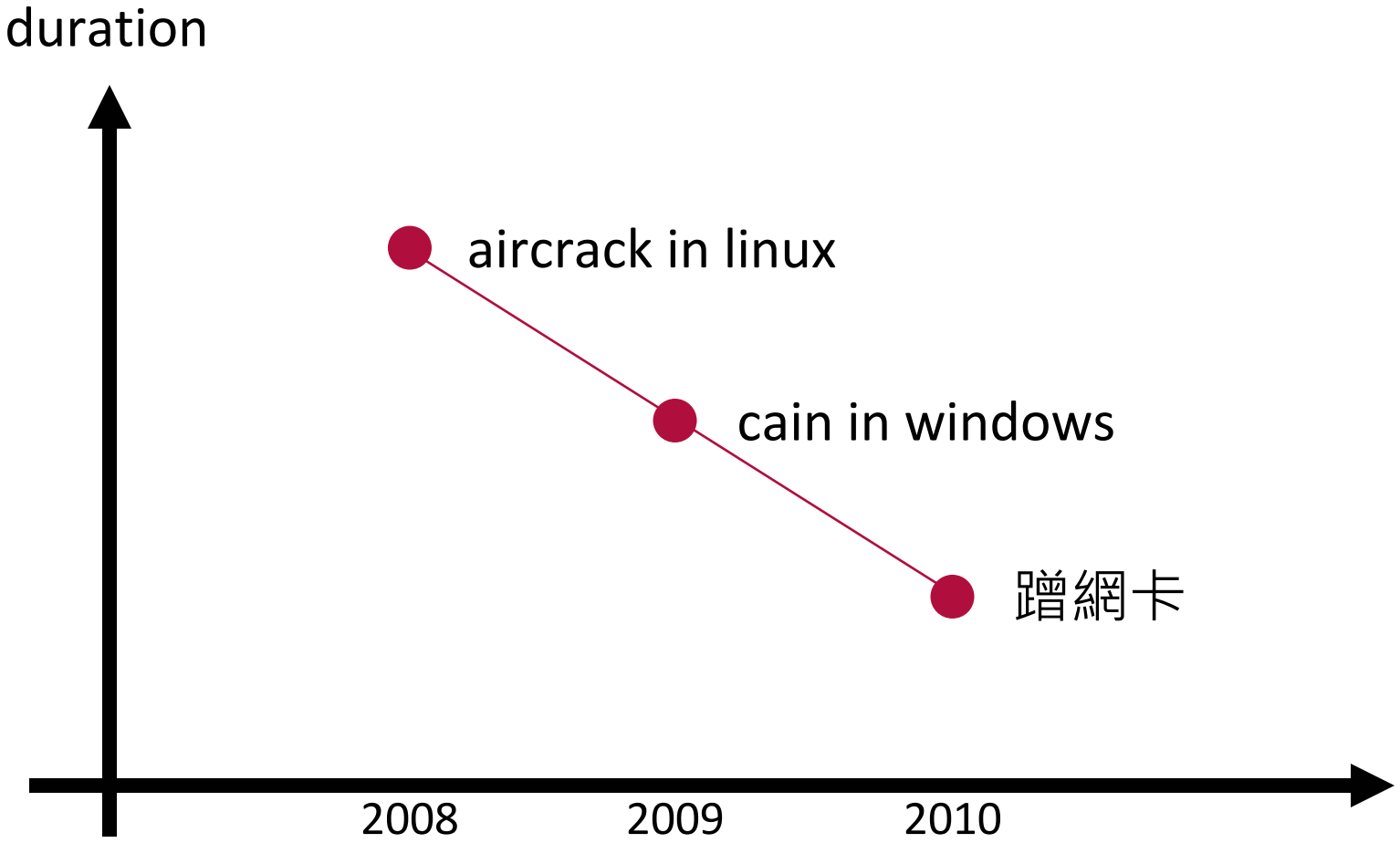
Demo 示範


SpoonWep 2 / Wep Finder / ShamanVirtuel 2K8
SPOONWEP SETTINGS
VICTIMS DISCOVERY
HELP /HINTS
NET CARD
RAUSB0
DRIVER
ATHEROS
MODE
UNKNOWN VICTIM
NEXT

History of WEP Cracking



History of WEP Cracking Demo



Latest Update of PSK Threat

PSK Security Threat

- Apply to WPA or WPA2
- Weak Password

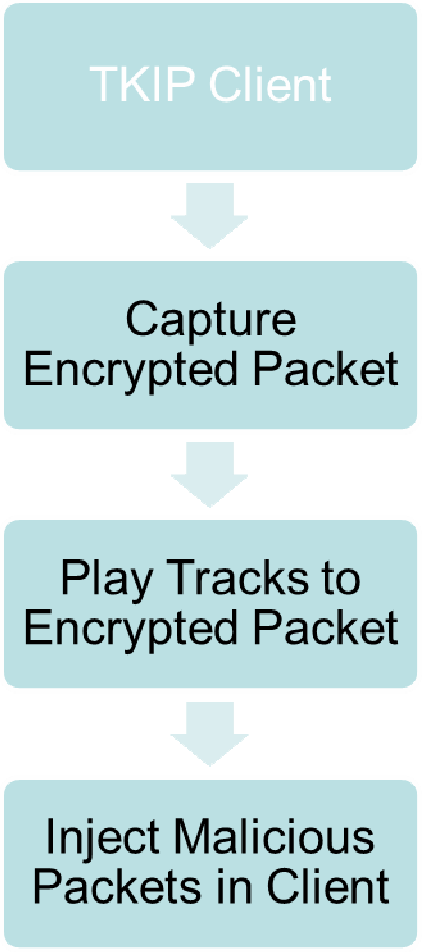
TKIP Weakness

TKIP Vulnerability

- Found in Year 2008
- Cannot crack the key
- Inject malicious packet
- Vulnerable if
  - Using TKIP and
  - Using 802.11e/WMM/QoS and
  - Long rekeying time: 3600 seconds or above

Software for Cracking TKIP

- Tkiptun-ng
  - Proof of concept tool
  - Develop
- Extremely Advanced Attack



Countermeasures

Countermeasure

- In Home & Small Environment
  - Using WPA/WPA2-PSK and **AES**
  - Good password
  - MAC Filter
  - Change SSID (**minimize the threat of rainbow table attack**)
  - Hide SSID (**makes PSK cracking difficult**)
- In Enterprise
  - Using WPA or WPA2 and **AES**
  - Change SSID
  - Hide SSID

Risk Level

No Encryption	→	Critical
WEP	→	High
WPA/WPA2 PSK	→	Medium
WPA/WPA2 TKIP	→	Medium
WPA AES	→	Observation

Thank You