



# We Have Your WiFi Password

## Are Your Wireless Networks Secure?

Wireless networking has become standard in many business and government networks. Despite the growing security concerns of wireless networks, it is still here to stay as the utilization of wireless LAN technology steadily increases.

Especially for corporate networks that heavily depend on wireless networks for internal communications. Attackers can sniff and steal sensitive information in your network, gain unauthorized access to use the Internet connection to hog bandwidth or even worse, for malicious activities such as hacking and Denial-of-Service attacks.

What are you waiting for?

Let us help you start protecting your wireless networks!

“New security loopholes are constantly popping up because of wireless networking. The cat-and-mouse game between hackers and system administrators is still in full swing.”

- Kevin Mitnick



# Wireless Network Penetration Testing

LGMS Helps You Identify Gaps in Your Organization's Wireless Security Controls

## Our Solution

LGMS can help you conduct a wireless network penetration assessment to identify any gaps in wireless security controls within your organisation.

Whether you already have an existing wireless network or planning to deploy a new one, LGMS can enhance your environment to maximize radio frequency coverage while minimizing channel interference.

In addition, LGMS will make sure that your wireless network has the necessary security controls while providing consultation customized to your organization's business nature.

## Our Services Provided

- Low level assessment of wireless network AP configuration in public areas.
- Collection of data transmitted over the wireless network.
- Emulation of a determined attacker to assess WEP encryption.
- Full encryption review including execution of WEP key recovery tools.
- Brute force attack and audit on WPS, WPA, WPA2 protection scheme.
- Denial of service attack emulation to assess defensive strategy.
- Rogue Access Point discovery.
- Host based assessment of supporting infrastructure (ACS server, Radius Server, Domain server, etc.).
- Review of policy and procedures dictating use of wireless devices.

## Executive Reports

A detailed report will be presented with the main topics covered as below:

- Identification of Access Points
- Wireless Network Coverage
- Wireless Network Security Assessment

```
[00:19:00] 2579528 keys tested (2324.06 k/s)

Current passphrase: zwlterboom

Master Key   : FF F3 65 24 75 76 06 70 42 66 53 31 F9 00 BD 0F
              CF 92 16 F1 88 F0 CF 23 CC 56 A7 74 93 79 7A 09

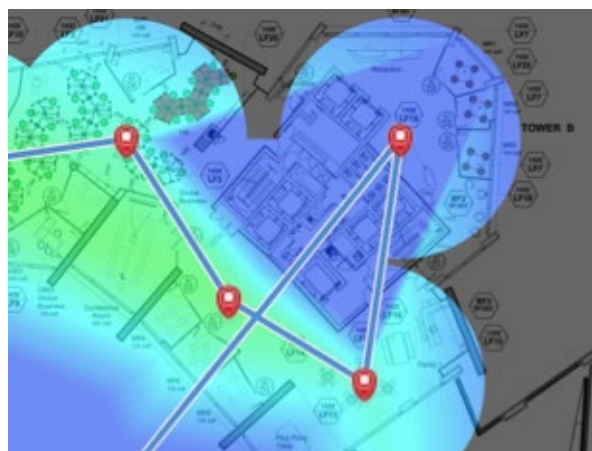
Transient Key : AE CB B9 BF 3B F7 43 87 D5 CF 0C 2C 43 23 79 01
              BE BA 43 34 26 B5 DF 6A 43 EC 4B EB A7 6D 61 B1
              5D 78 5C 1E 80 59 83 E3 FB 61 91 7F D1 85 AA A2
              B7 27 E7 37 03 FA FE 85 70 A5 18 E4 38 8E B4 E1

EAPOL HMAC   : 61 9A EA B7 1E 0D 58 79 30 94 85 D8 1C 47 EA DD

Passphrase not in dictionary

Quitting aircrack-ng...
```

Wireless Network Penetration Testing cover activities such as testing the protective measures on WPA / WPA2 / WEP / WPS.



Actual LGMS site survey report illustrating wireless signal quality

\* Governed by agreement between Client and LGMS

