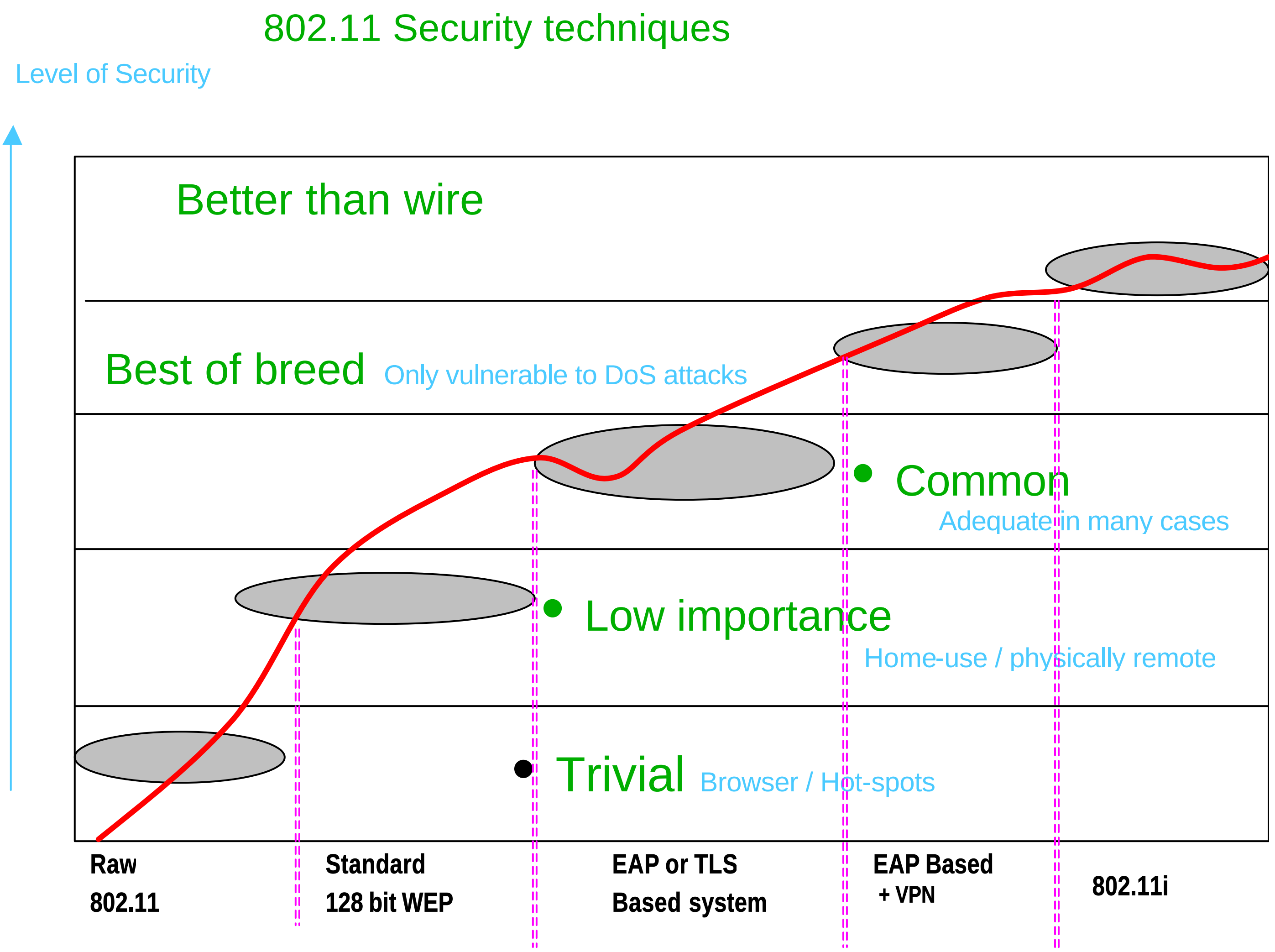
The 802.11 security method FAQ

A lot of people seem to be saying some very strange things about 802.11 security. I knocked out this document to help a little

1 A picture

To help reduce some of the confusion surrounding wireless security, I have produced this model.



2 Non-security

This table lists some of the common recommendations for wireless networks.

Overrated Counter-measures	Effect
Disable Broadcast SID	This can mean different things on different Access points. In any case, this isn't a solid security measure – it only reduces noise from casual passers-by. A countermeasure that discourages casual war-driving
Response to Probe/null probe	As above
DHCP	It is hard enough to run an enterprise network. The argument is that DHCP servers give out lots of hacker-useful info. But for anyone who has done ANY penetration testing they will know that any packet sniffer will reveal the IP address range in use, next hops for routing and DNS servers.
HEX/unprintable characters in the SID	Usually stops only valid users
VLANS & Firewalls	Not much security is provided by a VLAN. However, it can be use full to provide containment and group all Wireless connections together. Firewalls - I see this recommended often but again from people that don't think for a living. If you a not using a VPN, what on earth would the firewall rules look like and what protection would it provide! Don't forget IP addresses can be spoofed just like MAC addresses; so filtering by source address is pointless. And in most cases, the legitimate wireless users will need to access important HR or Fileservers – a good target for a war-driver.

3 Built-in security

Nearly all Access-Points will support some security features but they are very basic.

Type	Confidentiality	Authentication
WEP	Encryption is now readily cracked on a busy network	Poor - The WEP key is a shared secret shared for every device
MAC Filtering	Non-mac filtering provides no encryption	Poor - A simple packet sniffer will reveal if an association is rejected due to MAC filtering and what MACs are allowed Mac addresses can be changed on most cards

4 Additional security

If you are using Wifi for anything other than a home network or a hotspot, you should really consider using add-on security.

4.1 Why I don't recommend standalone VPNs anymore

Without strong server authentication, it is possible that a rogue access point could be used for a man-in-the-middle attack. This could be used to nullify the effect of an IPSEC layer-3 VPN.

The sequence of events is:

1) Client associates with local AP
2) Attacker dissociates it with fata_jack or WLAN_jack.
3) Client re-associates with a bogus AP
4) BOGUS AP associates with local AP

5) BOGUS AP forwards (modified) IP traffic from client to local AP

Then BOGUS AP can attack the IPSEC VPN in a number of ways. One way is to negotiate down the transformation methods used in phase 1 IKE negotiations. This could result in a AH-MD5 specification being used instead of (say) ESP-DES3. It could also could be used to change operation mode from envelope to in-place.

This isn’t a theoretical vulnerability – the *kracker-jack* vulnerability could be modified for use against many makes of VPN.

If the AP/server is authenticated the risk of these attack are reduced.

4.2 Add-on Security

Most security aware sites will try extra security – here is a summary.

Type	**Authentication Technique (Usual deployment)**	**Difficulty of Deployment**	**Standards Based**	**WEP Enhancements**	**Overall security**
MD5	one-way (Challenge based password)	Easy	RFC 1994 RFC 2284	no	Poor
TTLS	Mutual (Server via cert. client configurable)	Moderate	draft	per client/session generation	Better
PEAP	Mutual (Server via cert. client configurable)	Moderate	draft	per client/ session generation	Better
TLS	Mutual (Two-way cert. based)	Hard	RFC 2716	per client/ session generation	Good
LEAP	Mutual (Two-way challenge-based password)	Moderately easy	Proprietary	per client/ session generation Plus some integrity	Good

Type	Authentication Technique (Usual deployment)	Difficulty of Deployment	Standards Based	WEP Enhancements	Overall security
				improvements	
WPA	Mutual (Two-way challenge-based password)	Probably as easy as leap	Wifi Certified	per client/ session generation Improved some integrity (TKIP)	Good
802.11i	Mutual with 802.1x Plush secure Deauthentication & Disassociation	Unknown but probably similar to leap	Wifi Certified	encryption with AES and tkip	Very Good