# Where is the world heading when the Cyber World interferes with the Real World?

Cyber Forensics Computer Expert Simon Smith discusses the Danger of Remote Control Wi-Fi Tesla Cars

In response to recent media coverage exposing wirelessly hacking of a real Tesla motor vehicle, Simon Smith from www.evestigator.com.au is shocked to hear that the manufacturer is offering hackers bounty money to find further flaws in their security.

As a seasoned high-tech expert software developer first and foremost, any person in the industry understands how a systematic Software Development Life Cycle works. The testing phase is not left to the wilderness of hackers for reward, especially when the product is already on the consumer market and already has the ability to endanger lives. A software development company must have experts internally that can satisfy their customers internally.

For just $38 USD, one can purchase a WiFi extender device that will extend a simple signal for approximately 8 km at a dB level of approximately 200mw. I do not encourage this as this level is illegal in Australia. However my point is that technically any enthusiast can build a long range WiFi link over an extended line of sight peer to peer network offering various spoofed WiFi hotspots, not dissimilar to the method demonstrated in the recent article that shows 'Keen Security Labs' fooling the Tesla's auto-pilot system.

Tesla's comments that their "realistic estimate is that the risk to our customers was very low" in my opinion is not assuring enough. It is already known to consumers that Wide Area Networks exist in our major cities, offering internet access freely and that technology exists now rather cheaply for cyber hackers to spoof such networks that the Tesla vehicle (if following normal WiFi client protocol) may be broadcasting its presence to the outside world exposing itself.

Fake WiFi hotspots purporting to be trusted hotspots are a common hacking trick that is seen in cyber crime and phishing these days. The very nature of WiFi clients (unless purposely built against protocol) is to broadcast client beacons periodically through the air advertising their existence, and sometimes the existence of previous hotspots they have connected to. This in the past has been used to reverse engineer WPA2 security technologies and spoof existing networks by replicating their expected SSID purporting to be a "trusted connection".

An example of WiFi hotspot spoofing is as follows: Imagine being parked outside McDonald's, and connecting to a free McDonald's hotspot - but what you do not know is that you are connecting to a device held by a person in the car park and all your passwords and traffic are running through his eyes first in plain text before him.

In a vehicle situation, it is well known that a CAN bus of a modern day car is a 'local' Controller Area Network built inside the car, for that very purpose, and in my opinion has no purpose or place outside of that car. This flaw is a demonstration of when the "Cyber World interferes with the Real World". One thing consumers need to remember, and this is something I see everyday, is in the Cyber World, the controller is still a human or humans but we forget to focus on who is controlling and monitoring those humans?

The weakness in any computer information system is the human. In the Cyber World the human is unknown. We are going to see more and more cyber security risks like this that turn from augmented reality (like my PR on the dangers of Pokémon Go) to cyber reality like this. I have to say ladies and gentlemen, welcome to Cybergeddon. The line has been crossed and something needs to be done. Life is not a game, neither is our privacy or human rights. We should be concerned.

**Contacts**

Simon Smith
0410 643 121
mailto: forensic@evestigator.com.au