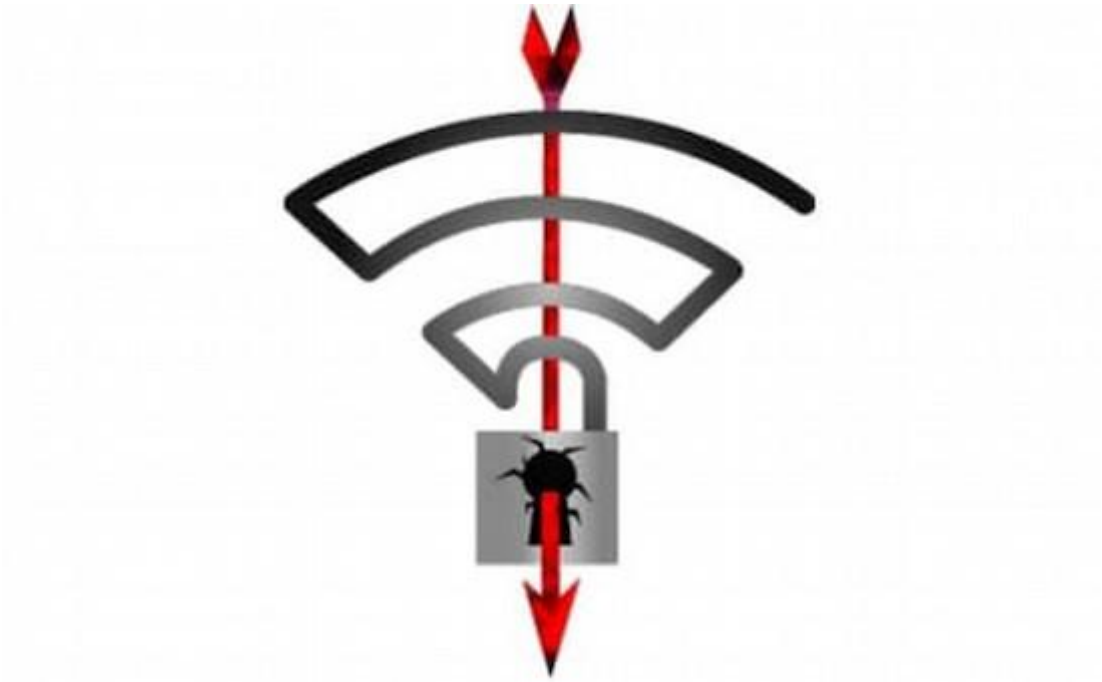
CIA has injected Wi-Fi network with risk of unprecedented 'Krack' hacking attack say European IT experts



The Krack Attack is the first flaw found in the WPA Wi-Fi encryption technique in 14 years

- By James Titcomb For The Telegraph

Every Wi-Fi connection is potentially vulnerable to an unprecedented security flaw that allows hackers to snoop on internet traffic, researchers have revealed.

The vulnerability is the first to be found in the modern encryption techniques that have been used to secure Wi-Fi networks for the last 14 years.

In theory, it allows an attacker within range of a Wi-Fi network to inject computer viruses into internet networks, and read communications like passwords, credit card numbers and photos sent over the internet.

The so-called "Krack" attack has been described as a "fundamental flaw" in wireless security techniques by experts. Apple, Android and Windows software are all susceptible to some version of the vulnerability, which is not fixed by changing Wi-Fi passwords.

"It seems to affect all Wi-Fi networks, it's a fundamental flaw in the underlying protocol, even if you've done everything right [your security] is broken," said Alan Woodward of the University of Surrey's Centre for Cyber Security.

"[It means] you can't trust your network, you can't assume that what's going between your PC and router is secure."

Most modern Wi-Fi networks have their traffic encrypted by a protocol known as WPA or WPA-2, which has existed since 2003 and until now has never been broken. This protects data as it travels from a computer or smartphone to a router, stopping hackers and spies from monitoring networks or injecting malicious code into the transfer.

Connecting to a secure network involves a four-way "handshake" between a device and a router to ensure that nobody else can decrypt the traffic. Researcher Mathy Vanhoef of the University of Leuven in Belgium found a way to install a new "key" used to encrypt the communications onto the network, allowing a hacker to gain access to the data. This could involve passwords, credit card numbers, photos and messages sent over a network to be stolen, or cyber attacks to be inserted into the traffic.

The attack cannot be carried out remotely, an attacker would have to be in range of a Wi-Fi network to carry it out. It would also not work on secured

websites - those that use https at the start of their web address instead of http.

Prof Woodward said that the only way to fix the flaw would be to manually replace or patch every router in people’s homes. He said that while the attack was not technically easy, tools would soon spring up allowing criminals to carry out the attack.

Related Topics

- Cyber attacks
- University of Surrey
- Viruses
- Internet security
- Internet