WPA2 (Wi-Fi Security) Has Been Hacked

Here is what we know so far as this story is still developing. A research firm[1] has discovered a weakness in the strongest known Wi-Fi security, WPA2 using a hacking technique called KRACK (Key Reinstallation Attacks).

It is important to note that only highly skilled hackers that are physically close (within 200ft) to your Wi-Fi network, could theoretically hack into your network.

Client Devices Are Vulnerable, Not Routers

Here is a blurb from the FAQ by the research firm that discovered the vulnerability:

Q What if there are no security updates for my router?
A Our main attack is against the 4-way handshake, and does not exploit access points, but instead targets clients. So it might be that your router does not require security updates. For ordinary home users, your priority should be updating clients such as laptops and smartphones.

In order to keep your data safe and secure, the primary focus should be on your client devices (ie: smartphones, tablets, laptops, and any other wireless devices like Wi-Fi thermostats, Smart TVs etc). Many companies that make these types of devices have already released updates and patches so that you can keep your devices secure. Once your Wi-Fi devices are updated, your network will be as safe as it was before this hack was discovered.

Where Can I Find More Info About This

We won’t go into the technical details of this hacking technique here but for more information directly from the man who discovered this vulnerability go to www.krackattacks.com

We Will Post New Firmware As Soon As Possible

Even though access points and routers are not the priority, we here at Mediabridge are still working on updated firmware versions for our Medialink routers. Routers do not have drivers or software updates like wireless clients do, but we are working on new firmware that would force client devices to use the updated WPA2 security. When we have a firmware update available for each of our routers it will be posted in the support section of each product’s listing:

New Firmware Will be Posted Here As It Becomes Available

MLWR-AC1200

MWN-WAPR300N

MWN-WAPR300NE

MWN-WAPR150Nv2

MWN-WAPR150N

1. Key Reinstallation Attacks: Discovered by Mathy Vanhoef of Imec-DistiNet.