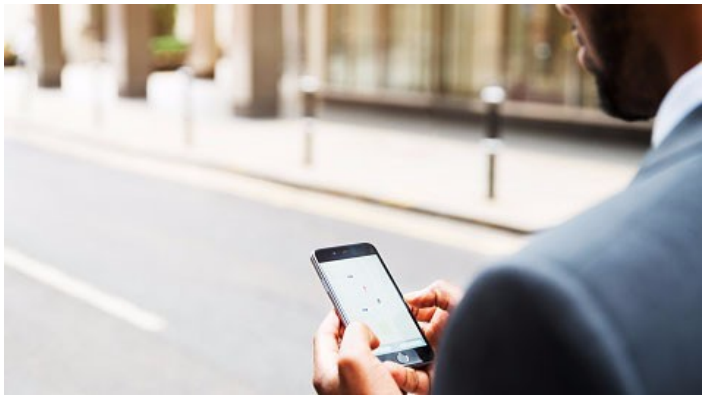
withersworldwide

Cyber threat named KRACK, impacting Wi-Fi networks and devices globally

03 NOVEMBER 2017

Allan Campbell
CHIEF INFORMATION SECURITY OFFICER | UK

CATEGORY:
ARTICLE



A new cyber threat named KRACK (Key Reinstallation Attack), impacting Wi-Fi networks and devices globally will gain wider media news and TV coverage. A critical design flaw in Wi-Fi technology used to secure wireless networks has been discovered. It is a flaw, which if exploited by nearby hackers, can potentially snoop and manipulate people's Wi-Fi communications over the air. There is plenty of information available on the Internet for those who are technically inclined.

Does this impact all devices I have at home and at work?

Think about all Wi-Fi enabled kit out there around the world and you can see why it is such a big concern. TVs, routers, fridges, sprinklers, baby monitors, heating systems, security cameras and kettles. Most of us use Wi-Fi connectivity for work, at home or whilst travelling.

Is that bad news for me?

Imagine if someone could view and then manipulate that device communication and insert new instructions into your now un-protected Wi-Fi communication, such as malicious nasty commands, against your vulnerable device. It could have alarming consequences in time if you could get a device to say overheat or switch off.

Can I use Wi-Fi in the office?

You can continue using Wi-Fi as normal at work. The vulnerability is new so no reported industry issues.

What if I work using Wi-Fi away from the office?

- Using Citrix connectivity for remote access to the office remains secure from laptops, home computers and from our new Mobile Device Management (MDM) solution. Citrix and MDM use different communication technology to secure information, even using Wi-Fi.
- Any web-sites visited starting with “https://” and displaying a “padlock” icon in the green address bar are considered safe. So banking and key retail sites access should be fine over Wi-Fi.
- If you have auto-updates for devices, consider enabling this functionality option.
- If you want super security over functionality then switch your Wi-Fi off and use your data. Unpopular cost implications, but I should mention it.

Any good news?

A big get of out jail card is that devices can only be manipulated if in Wi-Fi-range, which is a limited distance as you know when you walk around and lose your connectivity. So no manipulation is possible from far away like North Korea! A hacker in the coffee shop is a more likely scenario.

Now tell me what to do?

As with most technical vulnerabilities, the only way to fix it is through an update, known as a “patch” fix. This is produced by the manufacturers of the products and sent out to be updated and applied by you. What is more annoying is that iOS updates, Android, Windows updates for laptops, phones and tablets will be required. The big manufacturers are already working on it. Apple and Microsoft Windows have already released some fixes and Google for Android is coming soon. We will be patching business devices ongoing. Expect some e-mails or notifications from product manufacturers for personal Wi-Fi enabled devices in time as they catch-up.

In Summary, don’t panic but get updating when you can…

This is low risk but someone will find a way to exploit this Wi-Fi weakness in time. Let me know if you have any questions about this or any other security matters.

Authors

Allan Campbell

CHIEF INFORMATION SECURITY OFFICER | LONDON

Information technology

+44 20 7597 6303

allan.campbell@withersworldwide.com