Exploiting WPS-PBC on Windows 10

George Chatzisofroniou — @_sophron

35C3, 29th December 2018

Wi-Fi Association Attacks

Aka Man-in-the-Middle techniques on Wi-Fi

- They typically exploit a “usability over security” feature of the target OS

Most people know about KARMA and Evil Twin but there are others :)

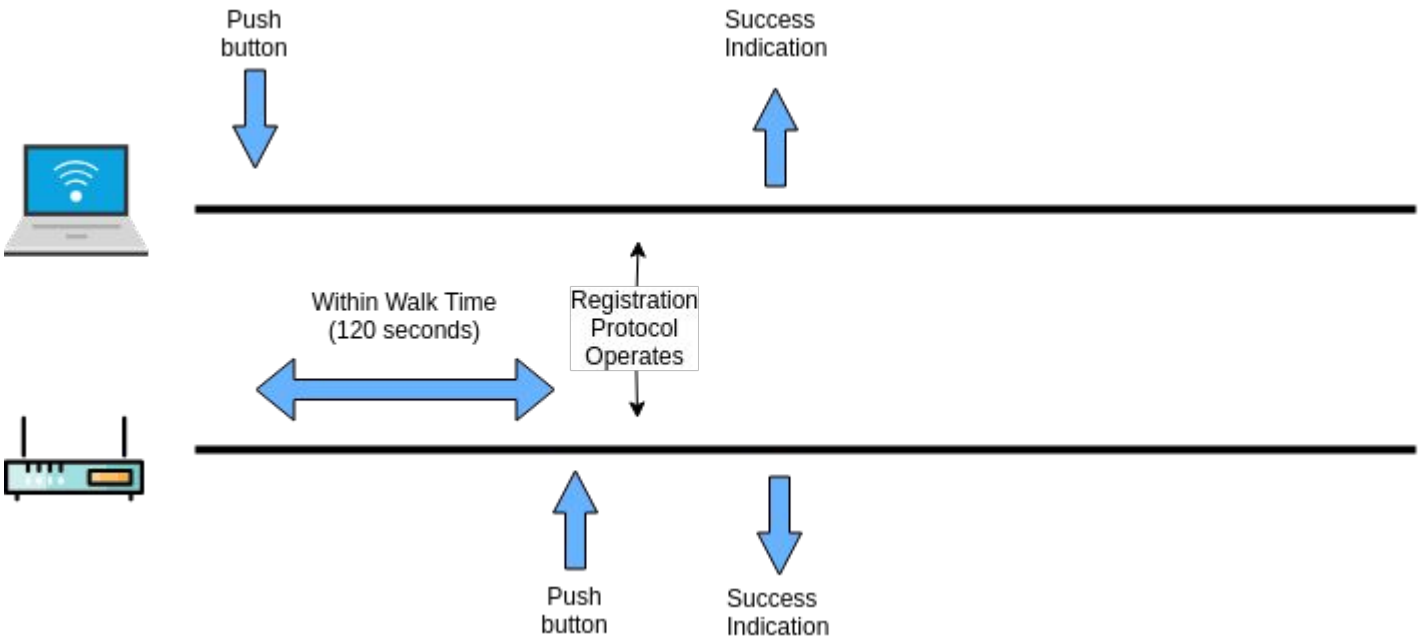
- In this talk: how can we **exploit WPS-PBC to achieve Man-in-the-Middle position against Windows 10 devices**

WPS-PBC

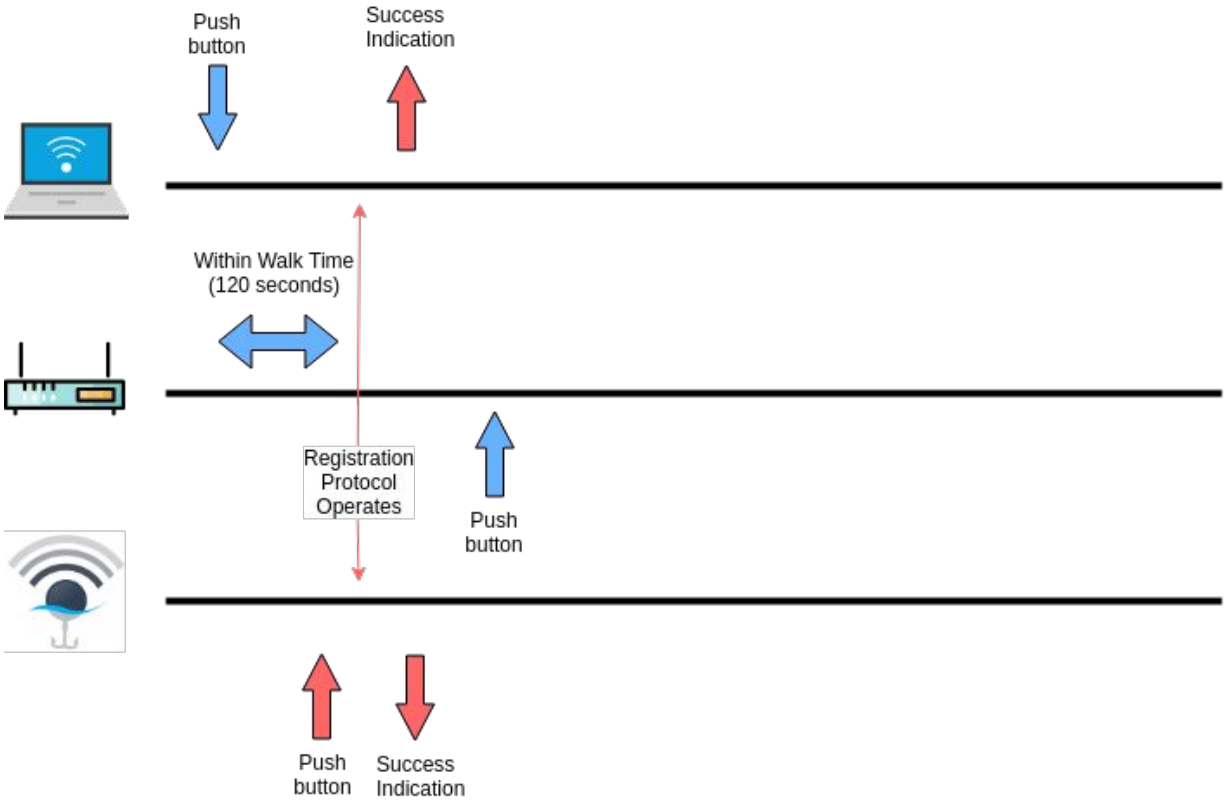
A network security standard making it easy to add new devices to an existing wireless network

- User presses a (virtual) button on the wireless device **and** a physical button on the router **within 120 seconds**
- Device automatically connects to the wireless network
- **No proper authentication mechanisms** in place

WPS-PBC


Push
button
Success
Indication
Within Walk Time
(120 seconds)
Registration
Protocol
Operates
Push
button
Success
Indication

What can go wrong?



The issue on Windows 10

“If I don’t use WPS-PBC, I am protected, correct?”

Even if you are not actively using WPS-PBC functionality, you are still **vulnerable if you are using Windows 10**

The issue on Windows 10

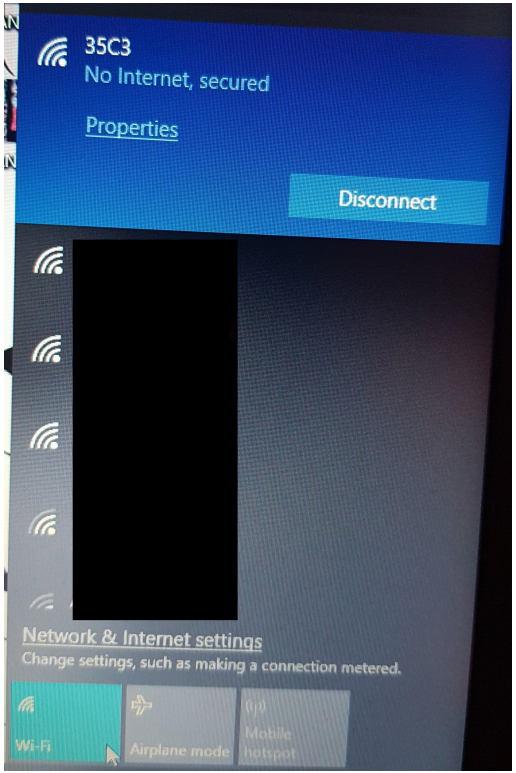
On Windows 10 selecting a WPS network **automatically pushes the WPS-PBC virtual button**

- You think you are not using WPS-PBC but you are!


A "USABILITY OVER SECURITY" FEATURE...
FOR ANOTHER "USABILITY OVER SECURITY" FEATURE

1. Victim is connected to a WPA/WPA2 network

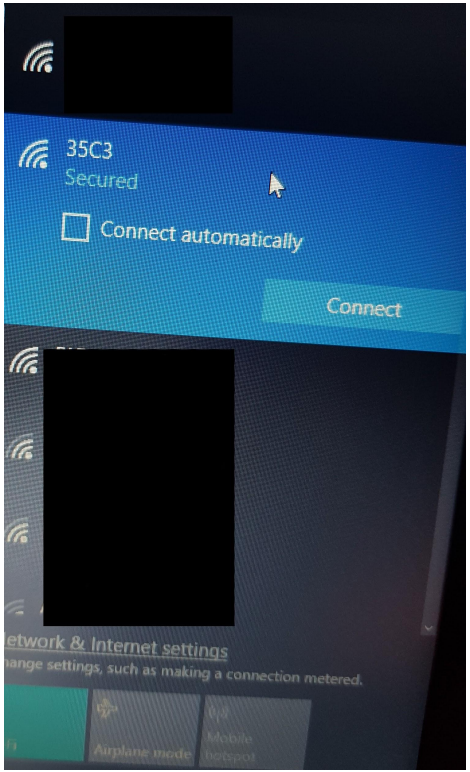
Victim is connected to a WPA/WPA2 wireless network with a Windows 10 laptop



2. Victim is disconnected from the network

We disconnect the victim from the legitimate network

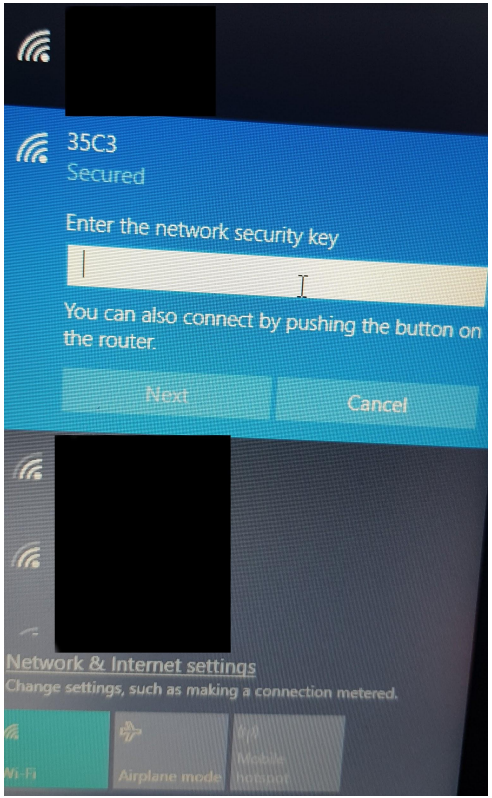
- E.g. using deauth/jamming techniques



3. Victim manually clicks on the network to re-establish the lost connection

We advertise the legitimate network BUT with WPS-PBC capabilities

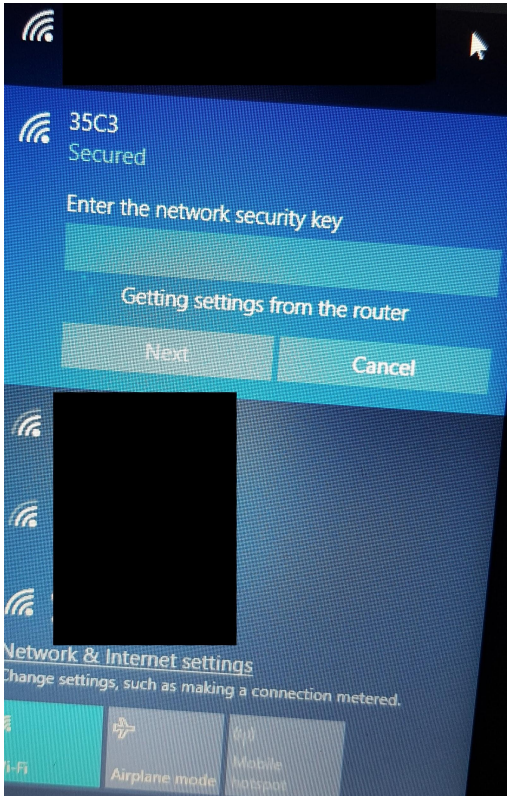
- Upon clicking on the network, the victim device automatically presses the WPS (virtual) button



4. Victim connects to our rogue AP

We press the button from our side as well :)

- Victim **connects to our rogue AP**
- It gives the impression of the “Auto-Connect” feature (e.g. because the victim had connected to the network in the past)



Thank you!

Twitter: @_sophron

Website: https://sophron.latthi.com