


# WPS+: how to fix it in a back compatible mode

 [linkedin.com/pulse/wps-how-fix-back-compatible-mode-roberto-a-foglietta](https://www.linkedin.com/pulse/wps-how-fix-back-compatible-mode-roberto-a-foglietta)



Published on April 25, 2016 -- Updated on October 18, 2016

The Wi-Fi Protected Setup (WPS) is a way to pairing two wireless devices pushing a button and sometimes inserting a personal identification number (PIN). Unfortunately the existing protocol implementation exchanges the PIN in two subsets which reduces greatly the guessing from 10 millions to 11 thousands.

Fixing a WPS vulnerability in a back compatible mode is possible changing only the router side. However, the most common objection is the well-know principle for which *the strength of a chain is determined by the weakest link*. In the same manner the security of a system depends on the weakest part. This is an analogy and it is useful to give us a broad picture but not to get deep enough into details and it may conduct us to a wrong conclusion that we should work on the both sides of the protocol implementation: false.

In WPS case, the weakest part is the router. The system A (R1, C1, C2, C3) and the system B (R2, C1, C2, C3) may have the same protocol, may have the same clients but have different level of security because the way in which the protocol is implemented into router R1 than R2. This happens any time there were multiple ways to implement a protocol maintaining the compatibility and in particular when the two ways differ because they are stateless and statefull.

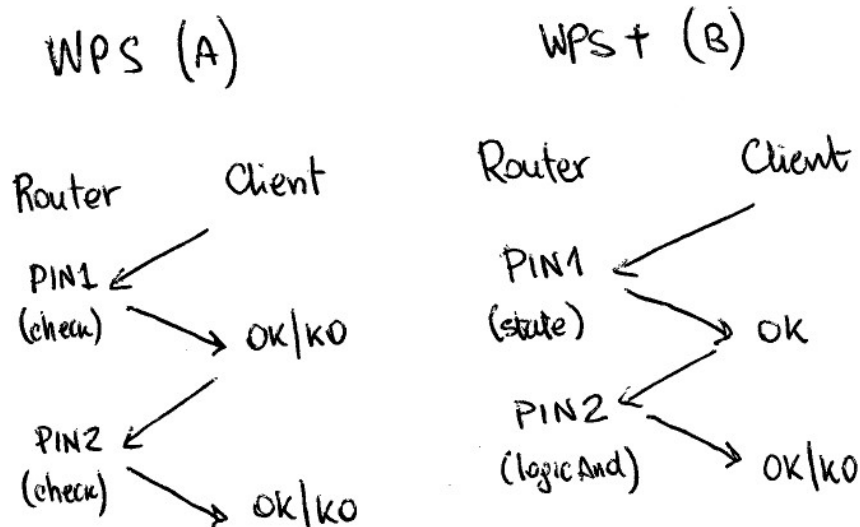
*When an enrollee attempts to gain access using a PIN, the registrar reports the validity of the first and second halves of the PIN separately. Since the first half of the pin consists of four digits (10,000 possibilities) and the second half has only three active digits (1,000 possibilities), at most 11,000 guesses are needed before the PIN is recovered. This is a reduction by three orders of magnitude from the number of PINs that would be required to be tested. As a result, an attack can be completed in under four hours. The ease or difficulty of exploiting this flaw is implementation-dependent, as Wi-Fi router manufacturers could defend against such attacks by slowing or disabling the WPS feature after several failed PIN validation attempts.*

-- Fonte: [https://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Setup#Vulnerabilities](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup#Vulnerabilities)

**The WPS is vulnerable because the router reports the validity of the first and second halves of the PIN separately.** Disabling the WPS feature after several wrong PIN submissions could have some good impact. However this approach may be not very effective if the defensive policy will delay only the second PIN half protecting the last 1.000 combinations, only.

The WPS+ would be less vulnerable even if it still exchange the PIN in two halves because the router reports always OK at the first PIN part challenge, even if the check failed, then it will report OK or KO as result of a logic AND of the two checks. In order to do that the WPS+ on router side

should be a statefull protocol implementation. It should keep memory of the previous first check result to deliver the final answer, later when the second challenge will arrive.



In such a way an attacker will not know if the first part of the PIN would be correct until it also found the correct second part of the PIN. So far, whatever reasonable way the client implements the protocol the entire system is enough strong to restore the initial 10 millions combinatory space.

Moreover a statefull implementation could be deliver a back compatibility WPS able to 1) be safer; 2) manage multiple WPS clients authentication in parallel; 3) have a more effective and selective brute force attack response policy. For all these reasons a complete statefull implementation of WPS deserve a specific name like WPS+, for example.

If you are interested in IoT pairing then take a look to [White Paper: IoT wireless pairing proposal](#) and fell free to contact me ([roberto.foglietta@gmail.com](mailto:roberto.foglietta@gmail.com)) for further information or in order to help you to develop your own implementation.

## UPDATE

May WPS could not be fixed in this way? Ok, then we found WHY we need a new protocol, HOW to implement it and WHAT should not be done (again). Is it right?

More question? From [Fare Innovatizione](#) (published in Italian on May 4th, 2016):

- if we have a manual then we use that manual, if we do not have a manual then we are going to solve a problem - *preferably* - before it will became a problem;
- we need to look at the big picture (holistic approach) before get deep into details;
- it is very important to make mistakes before going in productions, to learn something new from that mistakes;
- there are two kind of mistakes: those are wastes and those are teachers;
- for succeeding, we need to brilliantly choose our mistakes to make.

Developing the good questions is being half way from a good solution!

## Related article

- [White Paper: IoT wireless pairing proposal](#) (12 dicembre 2015, EN)