CNS HUT3

Information assurance

White Paper

WPS & False Prophets

By Andy Swift

16th January 2012

WPS Insecurities & False Prophets

There has been a lot of conversation throughout the start of this year among the security community about what WPS is and how it has provided hackers world wide with a simple and effective way to gain access to previously "secure" WiFi networks. Firstly we will be taking a closer look at the WPS technology itself and what it's fundamental vulnerabilities mean for individuals and organisations alike. Let's begin with a brief introduction to the technology itself.

Wi-Fi protected set-up or WPS as it is more commonly known is a standard that was created way back in 2007 by the Wi-Fi alliance. Their goal was simple: To provide secure and easy step by step router configuration for the average home user.

Wi-Fi enabled routers are now of course rolled out by most ISP's as part of a standard Internet package, their popularity has effectively skyrocketed over the last few years to a point where Wi-Fi enabled routers are now of course considered to be common place in the majority of households.

Unfortunately beyond a basic understanding of such technology, the majority of home users are blissfully unaware (through no fault of their own) as to the inner workings of a Wi-Fi router let alone how to configure it correctly and securely.

On many household routers the WPS feature leaves the factory enabled by default; it should be noted that to qualify for certification under the Wi-Fi alliance, which in itself has become a major selling point for home Wi-Fi routers, the feature must be present and enabled by default.

It's likely then that most home users will see WPS as an easy way to set their routers up in a secure fashion and also in many cases as a convenient way to quickly and securely add devices to their networks, usually via the touch of a button located on the front of the router.

It is interesting to read the original WPS specification from the Wi-Fi alliance and to note in particular that security was never really the main goal of the project, what appears to of taken it's place is a notable emphasis on providing a clean and user friendly experience to configuring a router.

So far, WPS would seem to be a great idea; an easy and effective way to configure and add devices to your home network that even the technically challenged would find to be a somewhat trivial task. However one should note that when creating a system to simplify a complex task more often than not simple is rarely the best practise or indeed secure.

Roll forward to December 2011 and a critical flaw was published to the public regarding the way users authenticate to a WPS enabled Wi-FI router. The flaw was identified and reported by Stefan Viehböck, who noted that when accessing the WPS service a user only needs to enter the 8 digit pin associated with the device (which is typically printed on the side of the router) to add devices to their network.

Company No. 03750954 VAT No. 728292808 Registered Office. 9 Wimpole Street, London W1G 9SR

As many readers will have noted already the implementation of this technology is...somewhat baffling; For example why are we encrypting everything on the network using proven and effective encryption technologies such as WPA or WPA2 with (presumably) super secure pre-shared keys when the network can in actual fact can be accessed and devices added using a simple 8 digit PIN code?

For those readers interested in the maths, an 8 digit PIN code in this case can be represented by 10^7 or to put it bluntly 10,000,000 possible digit combinations; the security conscious currently thinking 8 digits could be cracked in a bearable amount of time given enough processing power, are in for a further treat.

As some of the better mathematicians among us may have spotted there are 10^7 possibilities and not 10^8 as you might well predict given 8 digits, this is indeed due to the fact that the last digit of the 8 is in actual fact not a random digit at all but a checksum digit used for checking the correctness of the 7 previous digits making this the easiest digit to predict.

Worrying though this is, Viehböck went further in his investigation, informing us that the registrar (as shown below) actually submits the 8 digit PIN in two separate segments of 4 digits.

This of course means that now there are only around 10,000 possibilities for the first segment and because one digit from the second segment is indeed a checksum, it rounds up to a nice total of only 11,000 possible combinations to crack the PIN code.

Many will be asking why this simple error was ever made, and why are only 4 digits checked at any one time? The answer becomes apparent when observing the protocol in use in the following diagram:

Company No. 03750954 VAT No. 728292808 Registered Office. 9 Wimpole Street, London W1G 9SR

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 || Description || PK_E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 || N2 || Description || PK_R || Authenticator	
M3	Enrollee → Registrar	N2 || E-Hash1 || E-Hash2 || Authenticator	
M4	Enrollee ← Registrar	N1 || R-Hash1 || R-Hash2 || $E_{KevWrapKev}$(R-S1) || Authenticator	proove posession of 1st half of PIN
M5	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S1) || Authenticator	proove posession of 1st half of PIN
M6	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(R-S2) || Authenticator	proove posession of 2nd half of PIN
M7	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator	proove posession of 2nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator	set AP configuration

As we can see at no stage in the entire exchange is the complete 8 Digit PIN checked, in fact we can see that starting at M4, the first half of the PIN is checked, if this fails at any stage because the PIN is incorrect an EAP-NACK message is sent back to the client.

Therefore an attacker will simply have to look out for the emergence of the EAP-NACK message and note where it occurs:

- If the attacker receives an EAP-NACK message after sending M4, it becomes obvious that the 1st half of the PIN was incorrect.

- If the attacker receives an EAP-NACK message after sending M6, then the 2nd half of the PIN can be seen as incorrect.

Various tools have predictably surfaced over the last few months to exploit this issue, (such as Reaver developed by Tactical Network Solutions – Maryland) that will make short work of the WPS vulnerability by attempting every combination of PIN in a brute force style attack, and most PIN's will undoubtedly be cracked in around 2-4 hours using this rather crude but effective method.

So, what does this all mean to the unsuspecting home user? Well put simply any vaguely "secure" Wi-Fi network (and by that I mean WPA or even WPA2) that has been configured (or comes with) WPS will have unknowingly rendered the aforementioned secure encryption protocols irrelevant as the network can now be accessed by breaking a simple 8 digit PIN number.

Company No. 03750954 VAT No. 728292808 Registered Office. 9 Wimpole Street, London W1G 9SR

The flaws uncovered in the WPS protocol are quite illogical, to the point where suggested fixes become somewhat trivial, here are a few to get started:

- It has already been mentioned that at no point is the entire 8 digit PIN checked, if this was implemented at the M4 packet or thereabouts then the amount of possible combinations for the PIN will be increased dramatically and the attack will become far more time consuming.
- A sensible lockout should be implemented (it should be noted this has been introduced in a number of routers but by no means the majority) where the attacker is locked out after x amount of attempts. Once again this will greatly delay (but not nullify) the attack.
- Disable WPS altogether. Abandoning this technology is a shame, after all lets not forget the Wi-Fi alliance set out with the best of intentions – however good ideas do not always result in good implementations as is the case here.

The key factor in all of this would appear to be down to one thing: Simplification for the everyday user. And what's more, this is by no means the first (or I dear say the last) time in this type of error will be made.

As the world we live in becomes more complex, and specialist technologies work their ways into everyday life (WiFi, RFID bank cards, Satellites etc) there's a need for the technologies to become accessible and usable to all – unfortunately there is one key word missing here, and that is "understood" and as long as this key word is missing from the equation, technologies like WPS or similar in principle to WPS will always crop up from time to time in an attempt to make our lives easier, but not help us understand how they work or should be configured. A key fact to keep in mind is that when making complex things easier to use, there will always be an element of risk involved be it from the user or from the technology itself as in this case.

It would therefore seem that WPS is somewhat of a false prophet in many respects, some may be tempted to argue that in some ways users would be better off learning how to secure their Wi-Fi networks for themselves, but understanding these technologies and how to configure them correctly takes time and considerable effort for a complete novice. However perhaps the core fact here is that technologies such as WPA/WPA2 are complex for a reason: they are hard to break unlike a 8 digit PIN code.

Company No. 03750954 VAT No. 728292808 Registered Office. 9 Wimpole Street, London W1G 9SR