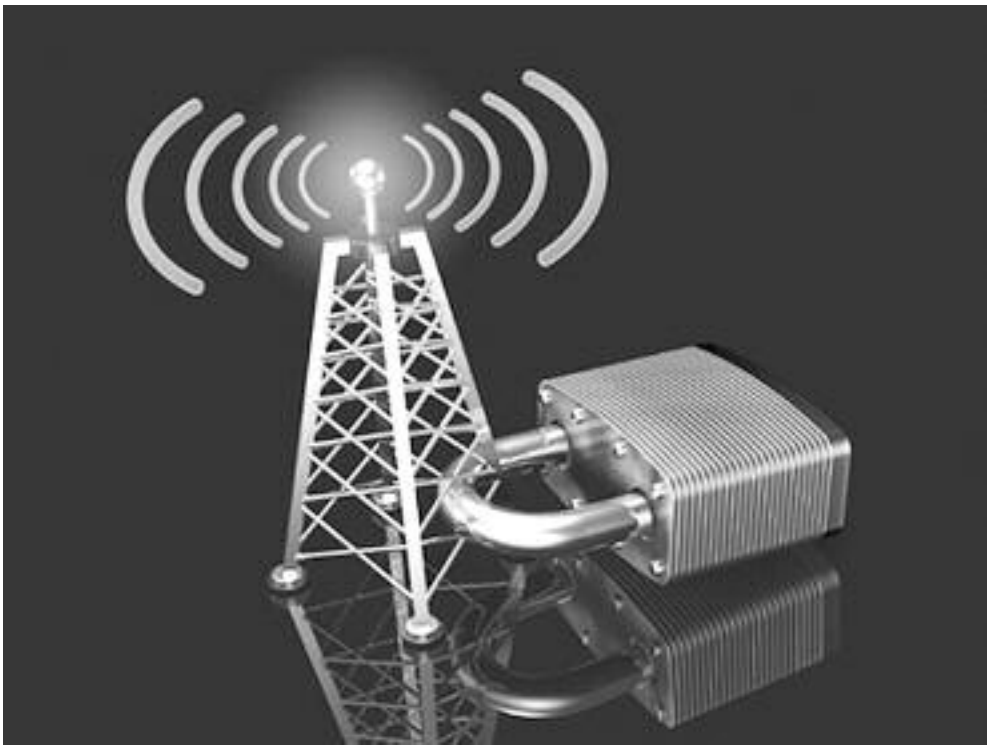
WiFi Continues to Have Serious Security Weaknesses

M J Morshed Chowdhury

Security in communication has been always a great concern. Different messages are sent constantly over the network whether they are simple correspondence between ordinary people, enterprise data or government secrets which all need to be kept secret. If you are using a Wi-Fi router to provide access to your home, business or customers (such as in a coffee shop), then you need to take action to protect your network from a recently discovered security weakness. Discovered late last year (2011) by Stefan Viehböck, this vulnerability in *Wi-Fi* Protected Setup (WPS) affects numerous Wi-Fi devices from a range of vendors. Details of the vulnerability have been made public; in other words, hackers know about it and will, no doubt, exploit it in unprotected systems.



Nowadays Wireless Protected Access (WPA) and it's improvement WPA2, which uses stronger primitives, are the most widespread solutions for wireless security. Wired Equivalent Privacy (WEP) is the predecessor of WPA and is considered to be deprecated however it still is in wide use.

WEP uses RC4 stream cipher for encryption and decryption. RC4 consists of Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA). KSA is used with concatenated 24-bit Initialization Vector (IV) and pre-shared key to initialize the state. PRGA uses that state to generate the stream which will be used to XOR together with the plaintext. IEEE 802.11 does not specify the selection of IV. Each WEP packet contains CRC-32 Integrity Check Value (ICV) which is supposed to indicate communication errors.

Over the years many weaknesses and attacks have been found for different parts of WEP. WEP was first broken by Fluhrer, Mantin and Shamir in 2001. ICV, which is included in ciphertext, do not actually provide information whether the packet has been tampered with or not. It indicates only transmission errors. Replaying packets is possible since WEP does not count packets. One of the first results on RC4 was by A. Roos who showed that there exists a class of weak keys that determine a large number of bits in KSA-s output (first permutation).

How Does the Wi-Fi Vulnerability Compromise Your Network?

WPS is a widely used means of easing the process of connecting to a Wi-Fi network, while still maintaining security. This protocol uses an eight-digit PIN to authenticate users. If you know your basic probability/counting theory, then you can easily calculate the number of possible PINs that a hacker has to choose from: 108 (eight digits, each between 0 and 9 inclusive). That's 100 million (100,000,000) possibilities. The 'brute force' method of attacking a WPS-protected Wi-Fi network is simply to try all the different combinations—a tedious process that can even take a computer a while to accomplish, given this number of variations. (Of course, the average brute force hack of such a network would take much fewer tries, but still somewhere near 50 million.)

In his investigation of the WPS vulnerability, however, Viehböck discovered that the protocol has design flaws that could greatly simplify a brute force attack. First, because the PIN is the only requirement for gaining access—no other means of authentication is required—brute force attacks are feasible. (If a username or some other means of identification was also required, for instance, then hacking the network would be much more complicated.)

Second, the eighth digit of the WPS PIN is a checksum, which the hacker can calculate given the first seven digits. Thus, the number of unique PINs is

actually 107 (seven digits), or 10,000,000 variations. But when performing authentication of the PIN, the access point (router) actually tells the potential client whether the first and second halves of the PIN are correct. In other words, instead of needing to find a single eight-digit PIN (actually, just a seven-digit PIN), a hacker need only find a four-digit PIN and a three-digit PIN (the second one includes the checksum). Again looking at the numbers, the problem thus reduces from finding one number among 10 million to finding two smaller numbers: one among 104 (or 10,000) possibilities and one among 103 (1,000) possibilities.

So, a hacker who wants to break into your (unpatched) network via your WPS-enabled Wi-Fi router need only try a maximum of 11,000 times—but on average, he would need to try only about 5,500 times. This is a far cry from the average 50 million or so attempts needed to hack the router were these design flaws unrecognized.

How Long Does It Take?

The other relevant factor in brute force attacks of this kind is how long it takes to attempt authentication. Even for only about 11,000 possibilities, if a single authentication takes several minutes, then the average hack could take days or weeks—nearly an eternity, particularly when gaining access requires physical proximity. (A customer in the coffee shop sitting there for a few days straight might draw attention to himself.) Needless to say, however, most users wouldn't tolerate such a long wait—according to Viehböck, a typical authentication takes between one and three seconds. A smart hacker could also take some measures to reduce that duration.

Assume that an authentication attempt takes 1.5 seconds. Given a maximum of 11,000 attempts, a hacker could gain access in about 4.5 hours or less—probably closer to 2 hours. A couple hours is certainly not a length of time that would draw attention in a coffee shop, or even in many other situations. And this type of attack is not exactly sophisticated (although some knowledge is required to do it efficiently): as the name implies, it is the equivalent of knocking the door down instead of picking the lock.

Who Is Affected?

This Wi-Fi vulnerability affects essentially any router that implements WPS security. According to the United States Computer Emergency Readiness Team (US-CERT), affected vendors include Belkin, Buffalo, D-Link, Linksys (Cisco), Netgear, Technicolor, TP-Link and ZyXEL. After identifying the PIN of the access point, a hacker could then "retrieve the password for the wireless network, change the configuration of the access point, or cause a denial of service," according to the US-CERT Vulnerability Note for this weakness. In other words, a hacker could potentially cause serious damage to your network.

Thus far, some vendors have provided more of a response than others. According to US-CERT, no practical solution to the problem is yet available, although some "workarounds" can mitigate the weakness to one extent or another. Certain routers, such as those from Technicolor, provide anti–brute force countermeasures to prevent hackers from gaining access: specifically, Technicolor states that its routers will temporarily lock out access attempts after a certain number of failed attempts (five retries). As noted in US-CERT's vendor information section for Technicolor, the vendor states that this feature prevents successful brute force hacks of the WPS-enabled router from being successful in less than about a week. Other vendors have responded differently to the problem, but no real fix to the problem has yet emerged.

What You Can Do in the Meantime

If a consumer lives in a house at the center of a 100-acre plot of land, he probably doesn't need to worry about his router being hacked. (Chances are, in this case, you don't even use a password.) Wi-Fi routers require a certain proximity to access the network, so by their nature, the scope of the problem is limited. Not everyone need worry about it. But if individuals not authorized to use your network (or who might abuse it) might be in range of his router, he needs to act.

Possibly the most effective means of protecting his network is deactivation of WPS. Even if he thinks he has disabled it, however, he may not has actually done so in some cases. Cisco hasn't offered a fix for the problem, Linksys routers could be vulnerable regardless of any steps he might take. A tool can be developed that allows anyone to test the security of his Wi-Fi router specifically with regard to this vulnerability. Beyond this action, he may have little recourse with his current router, pending further vendor action. Anti broute force attack should be impletemented to overcome this security vulneribility.

Conclusions

The Wi-Fi WPS vulnerability is just one more instance of how security flaws can enable hackers to harm your network, your privacy and your business. The battle will continue as hackers (or 'good guys') find vulnerabilities, vendors and protocol workgroups implement countermeasures, hackers find a way around the countermeasures and so on. To protect our network and our data, we need to stay up to date on security issues CJ

Source : Different Blogs