WPA2 wireless security cracked

March 20 2014

There are various ways to protect a wireless network. Some are generally considered to be more secure than others. Some, such as WEP (Wired Equivalent Privacy), were broken several years ago and are not recommended as a way to keep intruders away from private networks. Now, a new study published in the International Journal of Information and Computer Security, reveals that one of the previously strongest wireless security systems, Wi-Fi protected access 2 (WPA2) can also be easily broken into on wireless local area networks (WLANs).

Achilleas Tsitroulis of Brunel University, UK, Dimitris Lampoudis of the University of Macedonia, Greece and Emmanuel Tsekleves of

Lancaster University, UK, have investigated the vulnerabilities in WPA2 and present its weakness. They say that this wireless security system might now be breached with relative ease by a malicious attack on a network. They suggest that it is now a matter of urgency that security experts and programmers work together to remove the vulnerabilities in WPA2 in order to bolster its security or to develop alternative protocols to keep our wireless networks safe from hackers and malware.

The convenience of wireless network connectivity of mobile communications devices, such as smart phones, tablet PCs and laptops, televisions, personal computers and other equipment, is offset by the inherent security vulnerability. The potential for a third party to eavesdrop on the broadcast signals between devices is ever present. By contrast a wired network is intrinsically more secure because it requires a physical connection to the system in order to intercept packets of data. For the sake of convenience, however, many people are prepared to compromise on security. Until now, the assumption was that the risk of an intruder breaching a wireless network secured by the WPA2 system was adequately protected. Tsitroulis and colleagues have now shown this not to be the case.

If setup correctly, WPA2 using pre-shared key (PSK) encryption keys can be very secure. Depending on which version is present on the wireless device it also has the advantage of using strong encryption based on either the temporal key integrity protocol (TKIP) or the more secure counter mode with cipher block chaining message authentication code protocol (CCMP). 256-bit encryption is available and a password can be an alphanumeric string with special characters up to 63 characters long.

The researchers have now shown that a brute force attack on the WPA2 password is possible and that it can be exploited, although the time taken to break into a system rises with longer and longer passwords. However, it is the de-authentication step in the wireless setup that represents a

much more accessible entry point for an intruder with the appropriate hacking tools. As part of their purported security protocols routers using WPA2 must reconnect and re-authenticate devices periodically and share a new key each time. The team points out that the de-authentication step essentially leaves a backdoor unlocked albeit temporarily. Temporarily is long enough for a fast-wireless scanner and a determined intruder. They also point out that while restricting network access to specific devices with a given identifier, their media access control address (MAC address), these can be spoofed.

There are thus various entry points for the WPA2 protocol, which the team details in their paper. In the meantime, users should continue to use the strongest encryption protocol available with the most complex password and to limit access to known devices via MAC address. It might also be worth crossing one's fingers…at least until a new security system becomes available.

More information: "Exposing WPA2 security protocol vulnerabilities" in *Int. J. Information and Computer Security*, 2014, 6, 93-107. DOI: 10.1504/IJICS.2014.059797

Provided by Inderscience Publishers