Published on *Jisc community* (https://community-stg.jisc.ac.uk)

WLAN problems arising from the continued use of WPA / TKIP

Scott Armitage, Loughborough University

23 July 2010

In the early days of wireless networking, security was a low priority and therefore not very well designed or implemented. As a result, the Wired Equivalency Protocol (WEP) was seriously flawed and easily circumvented. It was soon realized that a more secure method of protecting communications was required for 802.11 networking. The solution came in the form of 802.11i, an amendment to the 802.11 standard, which introduced Robust Secure Networking (RSN). However as a solution was needed more quickly than the full 802.11i specification (WPA2) could be delivered, WPA was implemented as a stepping stone. WPA used the same RC4 cipher as WEP, to allow WEP based hardware to be software-upgraded, but was much more hardened against attack.

Over time, as wireless devices have been replaced with new ones, the number of WPA devices has decreased and the number of WPA2 has increased. This has led to a mixed environment with both protocols in use. However, one problem with mixed traffic (WPA and WPA2) on an Access Point (AP) lies in the Group Temporal Key (GTK). The GTK is an encryption key used to encipher multicast and broadcast wireless traffic. Each AP has only one GTK for all connected clients. This means the AP uses the lowest common denominator and therefore if a WPA/Temporal Key Integrity Protocol (TKIP) client joins, all WPA2/AES clients will drop to using a TKIP GTK (rather than Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)). Therefore a single TKIP client can reduce the security of every client on the AP.

The security is reduced as there are vulnerabilities in TKIP which allow an attacker to decrypt packets (but not obtain the pair-wise key used to encrypt: Practical attacks against WEP and WPA, Beck & Tews 2008). The likelihood of the attacks occurring is low as certain conditions need to be met to perform the attack. Even so, an attack which results in decrypted packets is possible and has been demonstrated. Rotating the pair-wise key more frequently (less than 120 seconds) can mitigate this attack, as this will prevent the attacker from being able to decrypt the full Integrity Check Value (ICV) in time before the key rotates. However, shortened re-keying times put an increased load on the RADIUS servers authenticating clients; additionally disabling sending MIC failure reports will also prevent the attack.

In addition to decrypting packets through exploiting TKIP, it is relatively trivial to perform a Denial of Service (DoS) attack on a wireless network. The primary problem stems from TKIP having no inherent defence against key-recovery attacks. Instead, as a protection mechanism, counter measures are taken. These countermeasures can easily be exploited to perform a DoS attack. The primary counter measure specifies that after two bad MICs within sixty seconds the AP must shutdown its radios for 60 seconds and then renegotiate its GTK and all pair-wise keys (A Study of the TKIP Cryptographic DoS Attack, Glass & Muthukkumarasamy 2007). This means an external attacker can invoke a 60 second shutdown by sending bad MICs, which can be achieved through a number of modification attacks (similar to those used to decrypt packets). Alternatively, a rogue authenticated client on the wireless network or a faulty client on the wireless network can initiate a 60 second shutdown trivially.

In addition to the security problems associated with TKIP there are also incompatibility issues with new technology. Whilst currently the majority of existing wireless deployments are 802.11a/b/g these are rapidly being replaced with 802.11n. The 802.11n standard does not support the use of WPA/TKIP. In 2009 the WiFi alliance amended their 802.11n certification process to prohibit the use of WPA/TKIP with 802.11n (CWNP Blog, No TKIP or No Certification: http://www.cwnp.com/index/cwnp_wifi_blog/5174 [1])

The above-mentioned problems can be mitigated. However, given that all wireless networking chipsets made since 2006 have supported WPA2 (Wi-Fi Certified Makes It Wi-Fi – An Overview of the Wi-Fi Alliance Approach to Certification, Wi-Fi Alliance 2006), the more secure solution is to move to WPA2/AES only. Through turning off the now legacy WPA, a much more secure and robust network is created without the need for tweaks to prevent known attacks. Indeed the WiFi Alliance is actively encouraging the removal of WPA/TKIP and from January 2011 are beginning to deprecate WPA/TKIP from their certification. The WiFi Alliance's plan is to have fully eradicated WPA/TKIP by 2014 (http://wifinetnews.com/archives/2010/06/say_goodbye_to_wep_and_tkip.html [2]).

Source URL: https://community-stg.jisc.ac.uk/library/advisory-services/wlan-problems-arising-continued-use-wpa-tkip

Links
[1] http://www.cwnp.com/index/cwnp_wifi_blog/5174
[2] http://wifinetnews.com/archives/2010/06/say_goodbye_to_wep_and_tkip.html