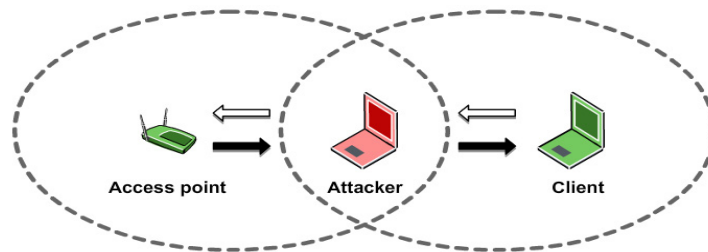


Update to WPA/WPA2 TKIP Exploit

A modification to the original TKIP attack is recently presented in a [paper](#) “A Practical Message Falsification Attack on WPA”, by T. Ohigashi and K. Mori, September 2009. This paper proposes two modifications as follows:

1. Requirement of multiple QoS streams traded for man-in-the-middle (MIM).

The basic idea here is to introduce MIM between the victim client and the AP which selectively drops packets transmitted to the victim client to create holes in client's sequence number counter. These holes are used by the attacker (collocated with MIM) to replay packets. This thus removes requirement of multiple QoS streams, which in the original exploit were needed for successful replays. The flip side is that a unique arrangement of devices is required in which the AP and the client cannot hear each other, but the attacker can hear both of them.



2. Some reduction in packet “injection” time.

First note that there is *no* decrease in lead time of about 12 minutes before any packet can be injected. Thereafter, only 1 falsified packet can be injected into client as there are no multiple QoS streams. In the success case (0.37 probability), it takes 1 minute to inject one falsified packet. Compare this to assured injection of 7 packets in 4 minutes in the original attack. The effective rate of packet injection is in fact more in the original attack.

Now if we combine the time reduction techniques of the new attack with QoS streams so that 7 packets can be injected per success, taking into account 0.37 probability of success, it is about 1.5 times faster. A further enhancement could be to inject both good and bad guesses (not described by researchers in the paper) which can then allow assured injection of 7 packets every minute and make it 4 times faster.

In summary, we do not think that the new discovery has much different impact compared to the original exploit. It proves existence case for the exploit in the absence of multiple QoS streams, but with stringent MIM requirement. It does not reduce 12 min lead time of the attack, but thereafter may increase the rate of packet injection somewhat.

For more information on WiFi security visit www.airtightnetworks.com.

To contact AirTight, email to sales@airtightnetworks.com or call +1 (877) 424 7844.