AIRTIGHT NETWORKS WHITEPAPER

WPA/WPA2 TKIP Exploit: Tip of the Iceberg?

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com

WPA/WPA2 TKIP Exploit: Tip of the Iceberg?

Both excitement and unease rolled through the wireless security community in November 2008 when news broke that researchers had cracked TKIP at the security convention in Japan [1, 2]. TKIP, an essential encryption component of WPA, which was heralded for years as the replacement for the broken WEP encryption to guard our wireless networks had been poked and sprung a leak for the first time.

A Review of WPA

WPA was introduced as a replacement for WEP around 2003. By 2003, WEP was completely broken which had a stifling effect on WLAN adoption. It was because of a timely effort on the part of the WiFi Alliance that WPA became available to replace WEP as a better security framework for WLANs.

WPA is a security framework whose: (a) encryption component is called TKIP, and (b) authentication component can be either PSK (designed for home users) or RADIUS (designed for enterprise usage). An important property of WPA, besides better security, was that WEP devices could be software/firmware upgraded to WPA. That is, they did not require a hardware upgrade. Since its introduction in 2003, WPA has served the purpose it was designed for very well and no vulnerabilities/exploits were discovered targeting enterprise WPA over last 5 years. Many organizations today have migrated to WPA as their wireless security framework.

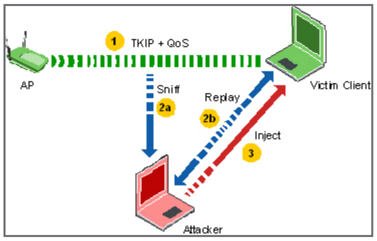
WPA Compromised for the First Time

And suddenly in November 2008, enterprise WPA was compromised for the first time with the discovery of the TKIP exploit. Below is the high level description of how this TKIP exploit works (see [1, 3, 4] for detailed technical description):

1) Victim: Victim of the TKIP exploit is any WLAN client connected to AP, which uses WPA for security and which also supports multiple QoS streams. The multiple QoS streams feature was introduced by IEEE 802.11e standard to facilitate supporting QoS sensitive voice over IP (VoIP) type of applications on WLAN.

2) Attack Vector: The attacker first passively sniffs wireless packets transmitted by the AP to such client and subjects the sniffed packets to combination of tricks such as replays and guesses.

3) Attack: When these tricks are completed, the attacker is able to wirelessly inject a certain number of arbitrary packets into the client.



The TKIP Exploit

Impact, Prognosis, and Remedies

In its current form, the impact of TKIP exploit is limited and there are some immediate remedies available to ensure that a WLAN does not fall prey to this exploit. The impact is limited because, in its current form, there are several limitations on what attacker can do with this exploit (see update on some of these points at the end of the paper):

I. First and foremost, it is not a key recovery exploit
II. It only works if client uses QoS feature of 802.11e/WMM
III. It is slow. There has to be lead time of about 12 minutes before any packet injection can be done. Thereafter, 7-15 packets can be injected every 4 minutes
IV. The injected packets have to be very small, say, less than 100 bytes
V. Packet injection in AP is not possible.

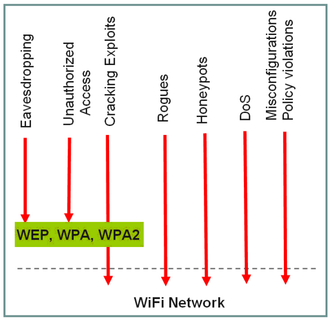
Nonetheless this exploit does provide hooks to build malware and attack sequences on top of WPA. Discussions have already begun in security forums on possibilities ARP poisoning, TCP manipulation, DNS manipulation etc. using this exploit. A concept attack sequence to inflict TCP indirection using this exploit to drill a hole in enterprise firewall is discussed in [4]. Moreover, discovery of exploits is an evolutionary process wherein one discovery leads to another. We have seen this happen in the case of WEP before, and history can repeat itself for WPA now that the first crack has developed. Given these possibilities, this development should not be ignored.

It is important to be proactive in protecting your networks from this exploit. Fortunately, there are antidotes available:

i) Turning off QoS feature: This remedy may only be practical for those enterprises which do not (intend to) support QoS sensitive applications such as VoIP over wireless.

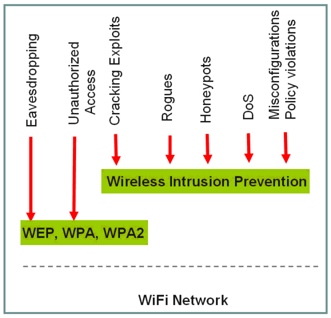
ii) Reducing TKIP key rotation interval: As a rule of thumb, this exploit can be frustrated by reducing TKIP key rotation interval to something less than 12 minutes (many enterprises currently use key rotation interval of 12 hours). The administrators however will need to evaluate the impact of this on performance of their APs.

iii) Wireless intrusion detection and prevention system (WIPS): Those enterprises which already have overlay WIPS installed and those which intend to install one in near future can seek protection from this exploit from their WIPS vendor. This exploit is detectable and preventable using overlay WIPS. For example, SpectraGuard Enterprise from AirTight Networks provides WPAGuard^{TM} feature to protect for such WPA exploits.



Single Layer Approach

iv) Migrating to WPA2: This exploit can be avoided by migrating to WPA2. WPA2 uses AES encryption instead of TKIP, thus eliminating exposure to TKIP exploit. This remedy is only possible for those which have WPA2 capable hardware and who are prepared to undertake the upgrade project right away. Unlike WEP to WPA transition, which was possible without change to WEP hardware, WPA to WPA2 transition requires hardware change.



Multi-Layer Approach

Note: WPA2 allows TKIP as optional encryption component. So migrating to WPA2 while continuing to use TKIP as encryption will not protect users from this exploit. They will have to use AES encryption with WPA2. Also the exploit is on TKIP encryption, so changing authentication component (PEAP, EAP-TLS etc.) of the security framework will not provide protection from this exploit.

Layered Approach to Wireless Security

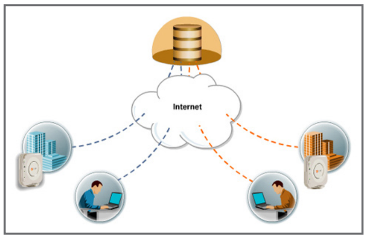
If you are wondering if migrating to WPA2 will solve the wireless security problem once and for all, unfortunately, the answer is a resounding NO. There is little doubt that WPA2 is a strong security framework which has: a) encryption component as AES (CCMP), and (b) authentication component either as PSK (designed for home users) or RADIUS (designed for enterprise usage). Nonetheless doors can be opened into WPA2 via misconfigurations, improper implementations and more importantly its combination with other protocols. In fact, recently an attack over WPA2 was demonstrated via misconfigured PEAP authentication component [5].

Today we are on the verge of embracing a new WLAN protocol, the much celebrated 802.11n. Much of WPA2 will run on 802.11n networks. The 802.11n is not battle-hardened in the field and might well have loose ends during the initial years of deployment. The possibility of these loose ends opening doors into WPA2 cannot be ruled out.

And finally, WPA2 is not even designed to address wireless threats from rogues, misassociations, honeypots, ad hoc connections, DOS attacks, MAC spoofing etc. So even if you deploy WPA2 in the network, the network still remains vulnerable to these threats. Hence, enterprises should deploy a second layer of security which can insulate them from both: a) Current and future cracking exploits, and b) other threats mentioned above. This second layer of security cover can be obtained by installing wireless intrusion prevention system (WIPS) in the network.

SpectraGuard Enterprise

WIPS can monitor your wireless environment for policy violations and suspicious activity which pose threat to wireless network. It can proactively alert on vulnerabilities in wireless networks which could be exploited by hackers. WIPS can also detect active threats. It can block wireless communication which in violation of enterprise wireless security policy and can also block active threats. It is also possible to physically locate source of vulnerability or threat using location tracking feature of WIPS. Additionally, WIPS can provide ongoing assessment and reporting on compliance of wireless networks to regulatory standards and best practices. Finally, as added benefit, WIPS can also facilitate monitoring of wireless network performance and troubleshooting of wireless network problems.



SpectraGuard Online

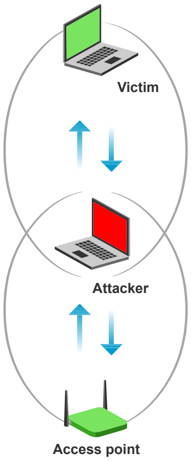
SpectraGuard WIPS from AirTight Networks

AirTight® offers wireless intrusion prevention (WIPS) in its SpectraGuard® product suite with both on site and on demand models providing a flexible, end-to-end solution that gives customers true visibility into their wireless security posture and a choice in how they manage it.

SpectraGuard automates every step of the wireless vulnerability management cycle so that you receive the network protection you need - from vulnerability assessment and compliance reporting to vulnerability remediation. You can have confidence in knowing that your information is protected over any wireless network and on any device. AirTight s the industry's first WIPS vendor with a comprehensive portfolio that helps protect, plan and optimize 802.11n networks.

If you would like more information about AirTight's solutions please contact: sales@airtightnetworks.com or Tel: +1 (877) 424 7844.

Update to WPA/WPA2 TKIP Exploit



A modification to the original TKIP attack is recently reported[7]. It 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 7-15 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 7-15 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 7-15 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.

References

[1] “Practical attacks against WEP and WPA”, by Martin Beck and Erik Tews, http://dl.aircrack-ng.org/breakingwepandwpa.pdf.

[2] “Battered, but not broken: understanding the WPA crack”, by Glenn Fleishman, http://arstechnica.com/articles/paedia/wpa-cracked.ars, November 06, 2008.

[3] Tkiptun-ng documentation: http://www.aircrack-ng.org/doku.php?id=tkiptun-ng.

[4] SANS presentation by Joshua Wright: https://www.sans.org/webcasts/show.php?webcastid=92188.

[5] “PEAP: Pwned Extensible Authentication Protocol”, by Joshua Wright and Brad Antoniewicz, ShmooCon 2008.

[6] “Is the latest vulnerability just the tip (or TKIP) of the iceberg?” Webinar by Pravin Bhagwat and Hemant Chaskar, PhD, AirTight Networks, http://www.airtightnetworks.com/home/news/events-and-webinars/webinar-tkip-vulnerability.html.

[7] “A Practical Message Falsification Attack on WPA”, by T. Ohigashi and K. Mori, http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf, September 2009.

ABOUT AIRTIGHT NETWORKS

AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry’s leading wireless intrusion prevention system (WIPS) and the world’s first wireless vulnerability management (WVM) security-as-a-service (SaaS). AirTight’s award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 12 U.S. patents and two international patents granted (UK and Australia), and more than 20 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit www.airtightnetworks.com

AirTight® NETWORKS