TECHNICAL BRIEF

Understanding the New WPA TKIP Attack

Vulnerabilities & Motorola WLAN Countermeasures

Executive Summary

On November 8, 2008, German researchers released a paper demonstrating a practical attack against the Temporal Key Integrity Protocol (TKIP) encryption algorithm used to secure Wi-Fi networks that are certified for Wi-Fi Protected Access (WPA). While the practical exposure from the attack is limited, it does lead to the decryption of small TKIP encrypted packets as well as injection of a few arbitrary frames from an adversary. This paper provides an overview of the vulnerabilities introduced by the attack as well as countermeasures available through the Motorola Wireless LAN solution to mitigate the new threat.

Attack Details

The original Wi-Fi encryption algorithm, Wired Equivalent Privacy (WEP), has significant flaws. Amongst other security problems, WEP is vulnerable to replay attacks. An adversary can capture and replay a WEP encrypted frame over and over again. This flaw is exploited by WEP attack tools such as "chopchop" that allowed a hacker to capture a WEP encrypted frame, replay the packet repeatedly, and decipher the payload one byte at a time. This method allows small packets like Address Resolution Protocol (ARP) frames to be decoded in 10-20 seconds without ever breaking the WEP key.

TKIP was introduced in 2003, and amongst other enhancements, included a new per packet hashing algorithm, the Message Integrity Check (MIC). MIC is based on a weak algorithm, designed to be accommodated on legacy WEP hardware. TKIP uses MIC for guaranteeing the integrity of an encrypted frame. If more than two MIC failures are observed in a 60 second window, both the Access Point (AP) and client station shut down for 60 seconds. The new TKIP attack uses a mechanism similar to the "chopchop" WEP attack to decode one byte at a time by using multiple replays and observing the response over the air. When a MIC failure occurs, the attacker can observe the response and waits for 60 seconds to avoid MIC countermeasures. Using the mechanism, the attacker can decode a packet at the rate of one byte per minute. Small packets like ARP frames can typically be decoded in about 15 minutes by leveraging this exploit.

TKIP also includes a sequence counter that could detect if a packet is being sent out of sequence. However, with the introduction of QoS based on the WMM standard, the sequence enforcement across multiple QoS queues was relaxed for performance reasons. This creates another security flaw. Once a TKIP frame has been decoded, the attacker can use the obtained key sequence to further inject up to 15 additional arbitrary frames using different QoS queues without triggering a sequence number violation that would have lead to the injected packet being dropped.

Summary of Vulnerabilities

1. This is not a key recovery attack. TKIP keys are not compromised and it does not lead to decryption of all subsequent frames.
2. The attack affects all TKIP deployments (WPA and WPA2) regardless of whether they use Pre-Shared Keys (PSK) or the more robust enterprise mode with 802.1x authentication.
3. The attack can reveal one byte per minute of a TKIP encrypted packet. Small frames like ARPs are good candidates for the attack.
4. If QoS is enabled, the attack can also lead to injection of up to 15 arbitrary frames for every decrypted packet. Potential attack scenarios include ARP decoding followed by ARP poisoning, DNS manipulation, etc.
5. WPA and WPA2 networks that use the more robust AES-CCMP encryption algorithm are immune to the attack.
6. The attack is capable of decrypting a TKIP frame sent from an AP to a station (not station to AP).

Motorola WLAN Countermeasures

The Motorola WLAN solution consists of several countermeasures already built into the product to mitigate the new TKIP attack. Motorola recommends that enterprises use AES-CCMP encryption with their WPA or WPA2 deployments. Motorola WLAN infrastructure is fully certified for AES-CCMP. Organizations that have legacy client devices that cannot support AES encryption and rely on TKIP have the following additional safeguards that they could use.

TKIP Key Rotation

Motorola WLAN infrastructure supports TKIP key rotation. Broadcast keys can also be periodically rotated. Forcing more frequent key rotation will limit how much plaintext can be derived by a hacker since each minute of key life can be used to determine a byte of plaintext using the attack.

```
(config-wireless)# wlan <WLAN> dot11i
key-rotation enable

(config-wireless)# wlan <WLAN> dot11i
key-rotation-interval <SECONDS>
```

The Motorola WLAN also supports periodic 802.1x re-authentication.

```
(config-wireless)# wlan <WLAN> radius
reauth <SECONDS>
```

If QoS is not really needed, the WLAN administrator has the option to explicitly disable QoS on the Motorola WLAN thereby preventing further injection attacks even if a TKIP frame is decrypted.

```
(config-wireless)# no wlan <WLAN> qos
classification wmm
```

Monitoring and Logging

The Motorola WLAN logs station MIC failures. A suspicious sequence of a single MIC failure reported by a single station every minute for several minutes would indicate that the TKIP attack is in progress. The syslog message generated by the Motorola WLAN for a MIC failure is as follows:

```
"Station [MAC_ADDR] reported a TKIP
message integrity check fail on wlan
[WLAN_ID]"
```

Motorola AirDefense Wireless Intrusion Prevention

The Motorola WLAN solution features the industry leading AirDefense Wireless Intrusion Prevention System (WIPS). Motorola AirDefense WIPS capabilities also help contain the attack. The WIPS is capable of detecting MAC address spoofing that occurs when the adversary pretends to be an authorized device during the attack. The AirDefense WIPS can also detect replay attacks and trigger if a configurable number of injections in a set window of time exceeds a programmable threshold. The WIPS can generate an alarm, send SNMP traps to notify various security event management systems, alert an administrator via email/pager, etc. In addition, the offending device can be blacklisted, and all further frames from it are ignored for the blacklist timeout period.

MOTOROLA

motorola.com