A Survey of Attack Mechanisms on Infrastructure-Mode 802.11 Wireless Networks and Their Detection

Juan Manuel Madrid
Universidad Icesi, Colombia

INTRODUCTION

The 802.11 wireless network revolution has not come without trouble. Since their creation, wireless networks have been plagued with security problems, derived from poor initial design of 802.11 security mechanisms, accelerated deployment and adoption of the technology, and lack of user education.

The goal of this article is to present the reader with a survey of the currently documented detectable attacks to infrastructure-mode 802.11 wireless networks, and a proposal of mechanisms and metrics that can be used to detect such attacks. The attacks and their detection methods are divided in seven categories: Denial-of service, traffic analysis attacks, passive eavesdropping, attacks against WEP, attacks against WPA and WPA2 in pre-shared key (PSK) and Enterprise modes, and man-in-the-middle attacks.

BACKGROUND

This section presents an overview of the security mechanisms implemented in 802.11 wireless networks.

WEP (Wired Equivalent Privacy)

WEP was the first encryption scheme used in the 802.11 wireless networks (IEEE, 2012). Figure 1 shows how WEP encrypts each data packet.

WEP's most salient flaws are: (Borisov et al., 2001):

- The access point (AP) authenticates clients during initial handshake, but clients don't authenticate the AP at all. This means clients may be tricked into connecting to a rogue AP.
- WEP's key scheduling algorithm is not well designed (Fluhrer et al., 2001). Some IVs, known as weak IVs, reveal details about the WEP key. If enough packets with weak IVs are captured, their information makes it possible to guess the WEP key. Stubblefield et al. (2004) conceived the first practical attack exploiting this vulnerability, and Klein (2006) perfected the attack, allowing to perform it with less data.
- Since the ICV (integrity check value) is a linear function over the packet (CRC-32), an attacker can modify an encrypted packet, by using a bit mask that alters selected bits, and then patching the ICV using the bit mask's CRC-32.
- WEP does not protect against replay attacks.

WPA (Wi-Fi Protected Access)

WPA addressed the vulnerabilities of WEP (IEEE, 2012). Its main feature is TKIP (Temporary Key Integrity Protocol), a cipher suite designed to supplement WEP as follows:

- Per-frame key computation depends upon three factors: Transmitter's MAC address, a frame counter and a temporary key. In WEP, only the 24-bit IV was changed between frames. The counter protects against replay attacks.
- Each frame contains a message integrity code (MIC), which protects against address spoofing and frame modification. Encryption keys are renegotiated whenever these attacks are detected.
- WPA also implements mutual authentication between AP and client.

DOI: 10.4018/978-1-4666-5888-2.ch413

Figure 1. Overview of the WEP algorithm

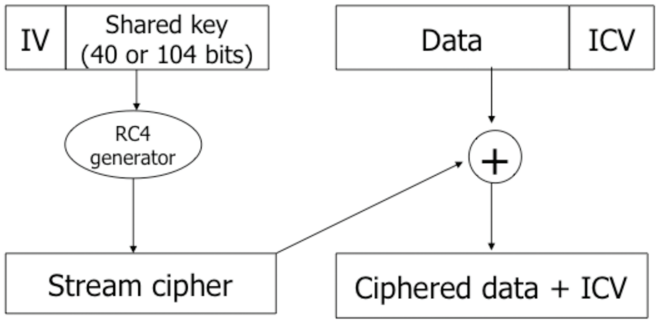
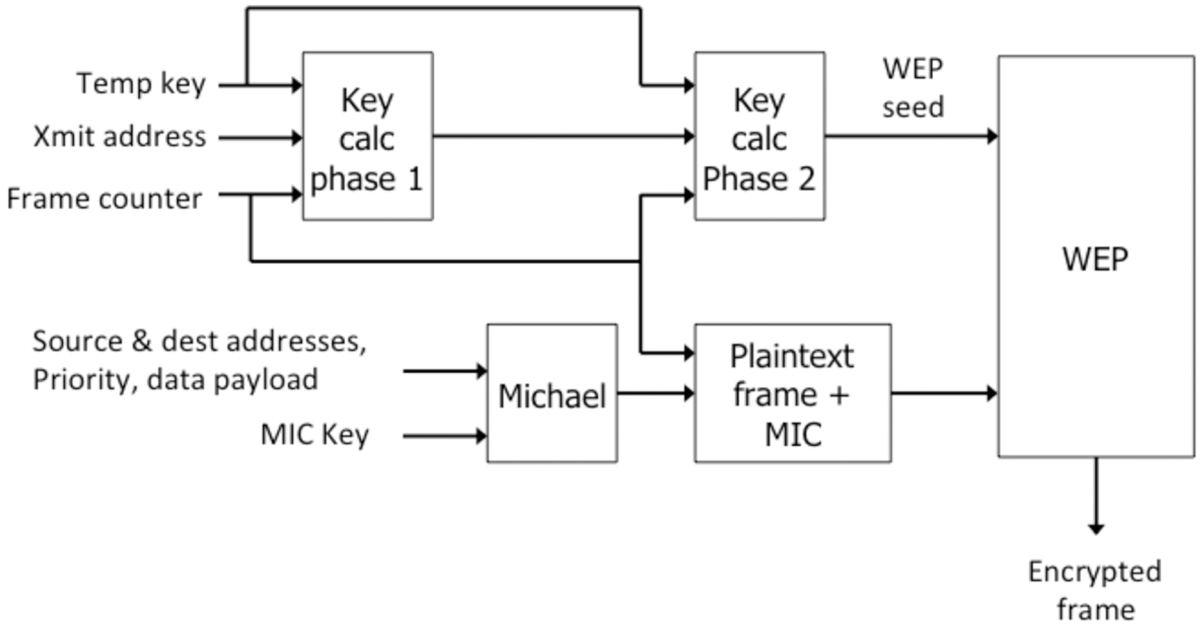


Figure 2. Overview of the TKIP algorithm



When operating in pre-shared key (PSK) mode, clients and AP share a passphrase. The devices then compute a 256-bit shared key using the PBKDF2 function (RFC2898, 2000). The ESSID is included in the shared key calculation, to protect against spoofing attacks.

Figure 2 shows the operation of the TKIP algorithm.

WPA2 was introduced in 2004. WPA2 replaces TKIP and mandates the usage of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). CCMP provides confidentiality (using AES encryption), authentication and integrity.

During the initial handshake, wireless client and AP negotiate a pairwise temporary key (PTK), used for unicast traffic, and a group temporary key (GTK), used to process broadcast / multicast traffic.

WIRELESS ATTACKS AND THEIR DETECTION

Denial-of-Service Attacks

The goal of a denial-of-service (DoS) attack is to prevent legitimate users from accessing the network and its resources. According to Potter and Fleck (2002), there are two types of DoS attacks: Radio jamming attacks, and network flood attacks.