How To Hack Wifi Wep Key Secured Network

The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types

April 14, 2010 - *PRLog* -- The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Reassociation Requests. Recall that management frames are always in the clear, even when WEP is enabled.

On a number of APs, it is possible to configure so that the SSID transmitted in the Beacon frames is masked, or even turn off Beacons altogether. The SSID shown in the Beacon frames is set to null in the hope of making the WLAN invisible unless a client already knows the correct SSID. In such a case, a station wishing to join a WLAN begins the association process by sending Probe Requests since it could not detect any APs via Beacons that match its SSID.

If the Beacons are not turned off, and the SSID in them is not set to null, an attacker obtains the SSID included in the Beacon frame by passive scanning.

When the Beacon displays a null SSID, there are two possibilities. Eventually, an Associate Request may appear from a legitimate station that already has a correct SSID. To such a request, there will be an Associate Response frame from the AP. Both frames will contain the SSID in the clear, and the attacker sniffs these. If the station wishes to join any available AP, it sends Probe Requests on all channels, and listens for Probe Responses that contain the SSIDs of the APs. The station considers all Probe Responses, just as it would have with the non-empty SSID Beacon frames, to select an AP. Normal association then begins. The attacker waits to sniff these Probe Responses and extract the SSIDs.

If Beacon transmission is disabled, the attacker has two choices. The attacker can keep sniffing waiting for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID and sniff the SSID as described above. The attacker can also chose to actively probe by injecting frames that he constructs, and then sniffs the response as described in a later section.

The goal of an attacker is to discover the WEP shared-secret key (http://www.eastmobiles.com/index.php?option=com_content&v...). Often, the shared key can be discovered by guesswork based on a certain amount of social engineering regarding the administrator who configures the wireless LAN and all its users. Some client software stores the WEP keys in the operating system registry or initialization scripts. In the following, we assume that the attacker was unsuccessful in obtaining the key in this manner. The attacker then employs systematic procedures in cracking the WPA (http://www.eastmobiles.com/index.php?option=com_content&v...). For this purpose, a large number (millions) of frames need to be collected because of the way WEP works.

The wireless device generates on the fly an Initialization Vector (IV) of 24-bits. Adding these bits to the shared-secret key of either 40 or 104 bits, we often speak of 64-, or 128-bit encryption. WPA2 (http://www.eastmobiles.com/index.php?option=com_content&v...) generates a pseudo-random key stream from the shared secret key and the IV. The CRC-32 checksum of the plain text, known as the Integrity Check (IC) field, is appended to the data to be sent. It is then exclusive-ORed with the pseudo-random key stream to produce the cipher text.   The IV is appended in the clear to the cipher text and transmitted. The receiver extracts the IV, uses the secret key to re-generate the random key stream, and exclusive-ORs the received cipher text to yield the original plaintext.

Certain cards are so simplistic that they start their IV as 0 and increment it by 1 for each frame, resetting in between for some events. Even the better cards generate weak IVs from which the first few bytes of the shared key can be computed after statistical analyses. Some implementations generate fewer mathematically weak vectors than others do.

The attacker sniffs a large number of frames from a single BSS. These frames all use the same key. The mathematics behind the systematic computation of the secret shared key from a collection of cipher text extracted from these frames is described elsewhere in this volume. What is needed however is a collection of frames that were encrypted using “mathematically-weak” IVs. The number of encrypted frames that were mathematically weak is a small percentage of all frames. In a collection of a million frames, there may only be a hundred mathematically weak frames. It is conceivable that the collection may take a few hours to several days depending on how busy the WLAN is.

Given a sufficient number of mathematically weak frames, the systematic computation that exposes the bytes of the secret key is intensive. However, an attacker can employ powerful computers. On an average PC, this may take a few seconds to hours. The storage of the large numbers of frames is in the several hundred-mega bytes to a few giga bytes range.

--- End ---

Source	Cellphonetrackers
Industry	Technology
Link	https://prlog.org/10626877

Scan this QR Code with your SmartPhone to-
* Read this news online
* Contact author
* Bookmark or share online