Vulnerabilities of the 802.11-based WEP

The 802.11 standard for wireless network includes a Wired Equivalent Privacy protocol, used to protect link-layer communication from passive and active attacks. The standard stipulates the use of the RC4 stream cipher for encryption. As has been described in the paper, the WEP protocol has major security flaws, some due to the way RC4 is used for confidentiality of messages and some due to the inherent nature of the WEP standard.

The RC4 algorithm is based on an XOR-operation on the plaintext with a keystream derived from an initialization vector and a secret key. This provides fast encryption. Secret keys could be of varying length, but the initialization vector must be 24 bits long. Hence, a brute-force attack to break the secret key is computationally infeasible. For ease of administration and maintenance of wireless networks, all clients connected to a network use the same secret key. Suppose the same initialization vector (IV) is used to generate a series of messages, a drawback of stream ciphers can be exploited. By using two cipher messages that use the same key and IV, the XOR of the corresponding plaintext messages can be obtained. If one of the messages is a known plaintext, the other can be computed. The ease of computing other plaintext messages using a known one increases as the number of ciphertext messages that use the same IV and key. It would therefore be necessary to vary the IV for each message transmitted. This however leads to the problem of repeated instances of the same IV, since the IV is restricted to 24 bits. On an average, the IV from a wireless client can be expected to repeat in about 8 - 12 hours. Since the IV is sent in the clear, it is possible to scan for repeating IV's on the network. Two messages with the same IV present the same vulnerability as described before. It is possible for a persistent attacker to build a decryption dictionary, which can then be used for intercepting and decrypting messages and launch attacks easily. An efficient key management scheme needs to be enforced to overcome the current drawbacks. Clients could be required to use distinct keys, and these keys could also be periodically refreshed to prevent replay and known-plaintext attacks.

WEP uses a non-cryptographic checksum for message authentication, and this gives rise to another series of attacks that exploit the specific drawbacks of the checksum. It is possible to alter the messages and yet, the integrity check would not be able to detect the violation. The linearity of the XOR-function and hence, of the RC-4 is exploited to include a small change in the actual message, and a checksum corresponding to this change is included in the actual checksum. These changes can be made without the knowledge of either component of the original plaintext - the message or the corresponding checksum. The resulting ciphertext message would be accepted as if it were an unaltered message by the integrity checker. This vulnerability can be used in an attack that the paper calls IP redirection. By altering the destination IP addresses of the outgoing packets on the wireless network, the attacker can cause these packets to be sent to a rogue host. The changed address would go unnoticed due to the same reason described above. However, this particular attack is more involved since the change in the address must be deterministic.

A message injection attack may be carried out using a plaintext corresponding to a ciphertext intercepted from the network. The RC4 stream can be recovered from these two quantities, and this can be used to inject new messages into the network using the flaw that repeating IV's will be accepted. A special case of this attack can be used to spoof authentication messages from a wireless client, by injecting the encrypted challenge replies. It is possible to obtain known plaintexts by a reaction attack on base stations. Acknowledgements to TCP packets are monitored and used as a basis to modify the TCP packet checksums one bit at a time, since the packet is encrypted. By repeatedly changing the bit

pattern in the intercepted ciphertext and adjusting the corresponding CRC checksum, it is possible to deduce the plaintext.

As the paper has pointed out, several changes may be required to the WEP standard in order to make it more secure. Another solution is to employ virtual private networks to grant access to wireless clients to corporate networks. Direct access to the external network should be denied and all wireless traffic must be routed through the VPN.