

Summary: Intercepting Mobile Communications: The Insecurity of 802.11

Summary: In this paper, the authors discuss the many insecurities found in the 802.11 protocol and more specifically the WEP protocol. WEP or Wired Equivalent Privacy is used in 802.11 networks to protect the link-level data during transmission. WEP uses a shared key with the RC4 encryption algorithm to attempt to provide confidentiality, access control, and data integrity. The problem with WEP lies in the fact that it uses only 24 bit initial vectors with each encrypted packet and has no specified mechanism for secret key changing. After a certain amount of traffic, the IVs will start to be re-used and lead to the plain text of messages being able to be recovered. Another major problem with WEP is the CRC checksum that is calculated and appended to each message before being sent. The CRC-32 checksum is an error checking mechanism and not one for ensuring non-tampering of data (such as a MAC). This leads to cases where parts of the message can be changed while still producing a valid checksum. There're a several other types of attacks that can be extended off of this weakness, including gaining unauthorized authentication to an AP.

Contributions: This paper's major contribution is the vulnerabilities shown in exploiting the CRC-32 checksum of the WEP protocol. The authors show how the CRC can be exploited to allow for undetected message alterations that can be further used in cracking WEP.

Weaknesses: Weaknesses in a paper like this are hard to find because the authors are analyzing a protocol and pointing out weaknesses. It is like trying to find a weakness of someone's weakness of someone else. What I would like to point out is that the authors concentrate a majority of their work on exploiting WEP through the checksum vulnerability. While these attacks can work, they seem much harder to do than other types of methods can be used. A more effective method would be to use an ARP replay attack to continually replay ARP requests that the AP would respond to with changing IVs. This would allow for a quick gathering of reused IVs and give means for cracking the WEP secret.